

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

TETSUYA SHIROGANE

Application No.: 10/765,289

Filed: January 26, 2004

For: STORAGE APPARATUS AND  
ACCESS MANAGEMENT  
METHOD THEREFOR

Customer No.: 20350

Examiner: Unassigned

Technology Center/Art Unit: 2131

Confirmation No.: 2560

**PETITION TO MAKE SPECIAL FOR  
NEW APPLICATION UNDER M.P.E.P.  
§ 708.02, VIII & 37 C.F.R. § 1.102(d)**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

This is a petition to make special the above-identified application under MPEP § 708.02, VIII & 37 C.F.R. § 1.102(d). The application has not received any examination by an Examiner.

(a) The Commissioner is authorized to charge the petition fee of \$130 under 37 C.F.R. § 1.17(i) and any other fees associated with this paper to Deposit Account 20-1430.

(b) All the claims are believed to be directed to a single invention. If the Office determines that all the claims presented are not obviously directed to a single invention, then Applicants will make an election without traverse as a prerequisite to the grant of special status.

(c) Pre-examination searches were made of U.S. issued patents, including a classification search, a foreign patent database search, and a literature search. The searches were performed on or around January 10, 2005, and were conducted by a professional search firm, Mattingly, Stanger & Malur, P.C. The classification search covered Class 707 (subclass 1), Class 709 (subclasses 217, 219, 223, and 226), and 711 (subclasses 114 and 152).

Because of the large size of these subclasses, keywords were used to narrow of number of

03/07/2005 SSITHIB1 00000105 201430 10765289  
01 FC:1464 130.00 DA

documents returned. The foreign patent database search was conducted using Espacenet database and Japanese patent database. The inventors further provided two references considered most closely related to the subject matter of the present application (see references #7-8), which were cited in the Information Disclosure Statement filed on January 26, 2004.

(d) The following references, copies of which are attached herewith, are deemed most closely related to the subject matter encompassed by the claims:

- (1) U.S. Patent No. 6,363,067 B1;
- (2) U.S. Patent Publication No. 2002/0174307 A1;
- (3) U.S. Patent Publication No. 2003/0177239 A1;
- (4) U.S. Patent Publication No. 2003/0229690 A1;
- (5) U.S. Patent Publication No. 2004/0044744 A1;
- (6) U.S. Patent Publication No. 2004/0111391 A1;
- (7) Japanese Patent Publication No. JP 2001-265655; and
- (8) Japanese Patent Publication No. JP 10-333839.

(e) Set forth below is a detailed discussion of references which points out with particularity how the claimed subject matter is distinguishable over the references.

A. Claimed Embodiments of the Present Invention

The claimed embodiments relate to security management in a storage system allowing a host computer to make accesses to data stored in a storage apparatus.

Independent claim 1 recites a storage apparatus for processing a command transmitted by a host computer connected to the storage apparatus by a network. The storage apparatus comprises a storage unit for storing data to be processed in accordance with the command; a memory for holding an access management table for storing first information on identification of the host computer; a first determination means for determining whether or not a frame of a login request transmitted by the host computer includes second information on identification of the host computer; a request means for transmitting a request to a source address specified in the frame of the login request in order to request the host computer to transmit the first information on identification of the host computer in a case where the determination result output by the first determination means indicates that the frame of the

login request does not include the desired second information; and a second determination means for carrying out a determination process on the first information transmitted by the host computer in response to the request issued by the request means by examination of the access management table. A decision as to whether or not to approve the login request is made in accordance with the determination result output by the second determination means.

Independent claim 10 recites an access control management method for managing an access permit for an access request transmitted by an external apparatus to a storage apparatus by way of a network. The access control management method comprises receiving a frame of a login request from the external apparatus in the storage apparatus; determining whether or not the received frame includes second information for identifying the external apparatus in a first determination process; requesting acquisition of first information for identifying the external apparatus from the external apparatus in a case where a result of the first determination process indicates that the frame does not include the second information; checking the acquired first information in a second determination process in order to determine whether or not an access permit should be given to the external apparatus; and approving an access request made by the external apparatus as a request for an access to the storage apparatus in a case where a result of the second determination process indicates that an access permit should be given to the external apparatus.

Independent claim 17 recites an access control management method for managing access permits for accesses made by a first apparatus as accesses to a second apparatus connected to the first apparatus by a network. The access control management method comprises acquiring predetermined first information from the first apparatus serving as an initiator of a communication in a case where the communication is determined to be unimplementable through the network in a first check mode of determining whether or not an access made by the first apparatus as an access to the second apparatus is an access made through the network by checking second information transmitted from the first apparatus to the second apparatus; and processing a command transmitted by the first apparatus to the second apparatus if an access requested by the command is permitted in a second check mode of determining whether or not an access made by the first apparatus as an access to the second apparatus is permitted by checking the first information acquired from the first apparatus.

Independent claim 20 recites a command-processing method for carrying out a communication between a first apparatus having an iSCSI initiator and a second apparatus having an iSCSI target through an IP network. The command-processing method comprises

receiving a frame of a login request made by the first apparatus in the second apparatus; checking whether or not the frame includes first predetermined information for identifying the first apparatus; issuing a request from the second apparatus for acquisition of second predetermined information for identifying the first apparatus from the first apparatus in a case where the frame does not include the first predetermined information; checking whether or not an access made by the first apparatus is to be permitted by examination of the second predetermined information transmitted by the first apparatus to the second apparatus; and processing a command transmitted by the first apparatus to the second apparatus in the iSCSI target of the second apparatus in a case where a result of checking indicates that an access made by the first apparatus as an access to the second apparatus is permitted.

Independent claim 22 recites a storage apparatus for executing a command received from a host computer connected to the storage apparatus by an IP network. The storage apparatus comprises a storage unit configured to store data to be processed by execution of the command; a memory configured to hold an access management table for storing first information on identification of the host computer; and a processing unit configured to process a request received from the host computer. The processing unit carries out a first determination process to determine whether or not a frame of a login request received from the host computer includes second information on identification of the host computer; transmits a request to a source address specified in the frame of the login request in order to request the host computer to transmit first information on identification of the host computer, and carries out a second determination process on first information transmitted by the host computer in response to the request by examination of the access management table in a case where a determination result output by the first determination process indicates that the frame of the login request does not include desired second information; and makes a decision as to whether or not to approve the login request in accordance with a determination result output by the second determination process.

One of the benefits that may be derived is that it manages accesses by improving security with regard to requests made by a host to make accesses to a storage apparatus adopting the iSCSI protocol.

B. Discussion of the References

1. U.S. Patent No. 6,363,067 B1

This reference discloses a staged partitioned communication bus for a multi-port bridge for a local area network. The communication bus is partitioned into a plurality of data bus segments. Each data bus segment is coupled to one or more ports of the multi-port bridge, and includes a same number (n) of signal lines. A staging multiplexer is coupled to each data bus segment and to a memory device. A bus controller is coupled to each port and to the multiplexer. Each port requests access to the memory device from the bus controller for storing data packets in the memory device and for retrieving data packets therefrom. In response to such requests, the bus controller conditions the multiplexer to provide a signal path between the memory device and the data bus segment that includes the requesting port. A look-up bus included in the multi-port bridge, which is operable independently of the staged partitioned bus, is preferably coupled to each port of the multi-port bridge and to a look-up table. The look-up table correlates destination addresses for data packets to identifications of destination ports. See, e.g., Abstract; Figures 1-22; and column 2, line 22 to column 3, line 55, and column 6, lines 20-49.

The reference does not teach determining whether or not a frame of a login request transmitted by the host computer (or external apparatus or first apparatus) includes second information on identification of the host computer, as recited in independent claims 1, 10, 17, 20, and 22.

2. U.S. Patent Publication No. 2002/0174307 A1

This reference shows a method for controlling secure access to storage devices attached to computer system networks. The system includes: a data storage device having the capability of comprising more than one storage structure; a switch comprising more than one port, wherein the ports are individually attachable to separate network systems and wherein the switch has the capability of receiving at one of its ports a request for access to one of the storage structures, and of identifying the network system making the request via the port at which the request was received; and an interface/controller connected to the switch and to the data storage device, wherein the interface/controller has the capability of receiving storage structure access requests from the switch and wherein the interface/controller has the capability of granting access to the storage structure requested if the identified network system making the request has authority to access that storage structure and otherwise has capability

of refusing access. The system also includes a port translation table that includes at least one entry comprising the identity of one of the ports and the identity of a virtual local area network specified as being attached to that port. See, e.g., Abstract; Figures 1-4; and paragraphs [0007]-[0010], [0021], [0038], and [0043].

The reference does not teach determining whether or not a frame of a login request transmitted by the host computer (or external apparatus or first apparatus) includes second information on identification of the host computer, as recited in independent claims 1, 10, 17, 20, and 22.

3. U.S. Patent Publication No. 2003/0177239 A1

This reference shows a method of managing a resource storage data, storage media having a resource managing program, and a resource manager for managing the resource storage data. The method includes receiving a resources allocation request across the network; converting the received resources allocation request into a setup request for network equipment that exerts control of the network; and sending the setup request to the network equipment or the storage systems across the network. If the resources allocation request designates an asset on an IP network, the request is converted into a setup request including the MAC address of the asset as an API parameter. This may include further steps of: under the control of the resources managing program, registering the following entries into a table: for each unit of the resources of the storage systems, its identifier on the network, its address which adapts to the type of the network, and a group identifier which is assigned by grouping the resources into allocation units; and allocating resources units making up a group in a lump, according to the group identifier. See, e.g., Abstract; Figures 1-9; and paragraphs [0010] and [0022]-[0031].

The reference does not teach determining whether or not a frame of a login request transmitted by the host computer (or external apparatus or first apparatus) includes second information on identification of the host computer, as recited in independent claims 1, 10, 17, 20, and 22. Nor does it disclose a specific request means for transmitting a request from the external apparatus to a source address specified in the frame of the login request.

4. U.S. Patent Publication No. 2003/0229690 A1

This reference discloses a secure storage system for securely accessing a storage device on a network and improving volume management scalability. The storage system includes a storage device and a client connected to a virtual private network using the

storage device. The system further includes: a management apparatus that manages the storage device by means of a logical volume assigned to the storage device; a conversion apparatus that converts a protocol corresponding to the storage device and a protocol used for the virtual private network; and a mapping means that stores a virtual private network allocated to the client and an access range of the storage device corresponding to the virtual private network. An iSCSI interface may be used for an access request from the conversion apparatus to the storage device. See Abstract; Figures 1-27; and paragraphs [0014]-[0019] and [0050]-[0066].

The reference does not teach determining whether or not a frame of a login request transmitted by the host computer (or external apparatus or first apparatus) includes second information on identification of the host computer, as recited in independent claims 1, 10, 17, 20, and 22.

5. U.S. Patent Publication No. 2004/0044744 A1

This reference shows methods, devices and systems for storage management in digital networks. The method provides a switch system having a first and second configurable set of processor elements to process storage resource connection requests, and to route the requests to at least one of the storage elements. Also included is a configurable switching fabric interconnected between the first and second sets of processor elements for: receiving at least a first storage connection request from one of the first set of processor elements; determining an appropriate one of the second set of processors for processing the storage connection request; automatically configuring the storage connection request in accordance with a protocol utilized by the selected one of the second set of processors; and forwarding the storage connection request to the selected one of the second set of processors for routing to at least one of the storage elements. The system has an IP data network including a network management system, a switch element, and at least one remote SCSI device attached to the switch element. A method of automatically discovering the remote SCSI device via the network includes: assigning, in the switch element, an IP address for the remote SCSI device; creating, in the switch element, an address resolution protocol (ARP) table including a table entry for the remote SCSI device; and the ARP table entry providing a mapping between the IP address and a physical address corresponding to the remote SCSI device. See, e.g., Abstract; Figures 1-46; and paragraphs [0017]-[0024], [0074]-[0081], and [0213]-[0216].

The reference does not teach determining whether or not a frame of a login request transmitted by the host computer (or external apparatus or first apparatus) includes second information on identification of the host computer, as recited in independent claims 1, 10, 17, 20, and 22.

6. U.S. Patent Publication No. 2004/0111391 A1

This reference discloses a command processing system by a management agent. In the system an ad hoc program is introduced that runs on a storage subsystem and which, upon receiving a management command from a system management computer, determines whether it should be executed or rejected, judging from the security level of the communication path from/to the system management computer and the security level required for the execution of the command. The system has a memory that stores a first table pre-registering the security levels of the communication path between the management application and the management agent; a first and second means of obtaining, for each command sent from the management application to the management agent, the operational security level for the command by referencing the first and second table; a third means of comparing the operational security level obtained by the first means and the required security level obtained by the second means; and a fourth means of determining whether to permit the execution of the command based on the result of the comparison made by the third means. See, e.g., Abstract; Figures 1-5; and paragraphs [0006]-[0007] and [0042]-[0048].

The reference does not teach determining whether or not a frame of a login request transmitted by the host computer (or external apparatus or first apparatus) includes second information on identification of the host computer, as recited in independent claims 1, 10, 17, 20, and 22.

7. Japanese Patent Publication No. JP 2001-265655

This reference discloses a technique to provide a security function in a storage subsystem by the flexible and efficient presentation method of storage resources by performing execution by high-speed judgment logic without affecting a processing on the side of a host computer. An information WWN for uniquely identifying the host computer, a management table where the correspondence of a logical unit number LUN inside the storage subsystem for which access is permitted to the host computer and a virtual LUN for presenting the LUN to be the access object to the host computer by a user optional method is described and the management table where the correspondence of the WWN and a



dynamically allocated management number S-ID is described are stored in a nonvolatile memory inside the storage subsystem beforehand. By retrieving the WWN of the host computer from the S-ID of the host computer and retrieving the accessible virtual LUN from the WWN, access propriety to the LUN inside the storage subsystem is judged.

In this reference, a relation between WWNs assigned to hosts and port IDs is stored in a table. For a frame including no WWN (e.g., a frame including CDB), the WWN for the port ID is examined to determine whether the host is allowed to make an access to the LU. Present application, at page 3, lines 3-8. In the IP network, however, information may be transmitted by way of a router. In this case, the MAC address included in a datalink frame is replaced with the MAC address of the network card of the router. Thus, if a router exists between the host and the storage apparatus, there is raised a problem that the target is not capable of acquiring the MAC address of the host from a packet received from the host. The reference does not describe a method of acquiring the MAC address of the host in a transmission through a router in the case of an MAC address used as an identification of the host in the IP network. Present application, at page 4, line 14 to page 5, line 1.

The reference does not teach determining whether or not a frame of a login request transmitted by the host computer (or external apparatus or first apparatus) includes second information on identification of the host computer, as recited in independent claims 1, 10, 17, 20, and 22.

8. Japanese Patent Publication No. JP 10-333839

This reference discloses a fiber channel connection storage controller having a security function for preventing any illegal access from a host device in an environment in which access from all of host devices can be physically accepted. N Port Name information for uniquely identifying a host device is set in a microprocessor 42 of a storage controller 40 before the starting of host devices 10, 20, and 30. When the host devices 10, 20, and 30 are stated, and an issued frame is received by the storage controller 40, the microprocessor 42 operates comparison to detect whether or not the N Port Name information stored in this frame is registered in an N Port Name list in a control table already set and held in the microprocessor 42, and continues a processing based on the instruction of the frame when they are made coincident, and rejects the request when they are not made coincident. Thus, any illegal access from the host device can be suppressed, and the security can be held.

In this reference, a table is stored in the storage apparatus in advance. For each LU, the table shows WWNs (World Wide Names) each assigned to a host allowed to make accesses to the LU. A WWN stored in a login frame received from a host is compared with those cataloged in the table to identify the host and to determine whether or not the host is allowed to make an access to the LU in the storage apparatus. Present application, at page 2, line 20 to page 3, line 2. In the IP network, however, information may be transmitted by way of a router. In this case, the MAC address included in a datalink frame is replaced with the MAC address of the network card of the router. Thus, if a router exists between the host and the storage apparatus, there is raised a problem that the target is not capable of acquiring the MAC address of the host from a packet received from the host. The reference does not describe a method of acquiring the MAC address of the host in a transmission through a router in the case of an MAC address used as an identification of the host in the IP network. Present application, at page 4, line 14 to page 5, line 1.

The reference does not teach determining whether or not a frame of a login request transmitted by the host computer (or external apparatus or first apparatus) includes second information on identification of the host computer, as recited in independent claims 1, 10, 17, 20, and 22.

(f) In view of this petition, the Examiner is respectfully requested to issue a first Office Action at an early date.

Respectfully submitted,



Chun-Pok Leung  
Reg. No. 41,405

TOWNSEND and TOWNSEND and CREW LLP  
Two Embarcadero Center, 8<sup>th</sup> Floor  
San Francisco, California 94111-3834  
Tel: 650-326-2400  
Fax: 415-576-0300  
Attachments  
RL:rl  
60417773 v1

## BEST AVAILABLE COPY

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-265655

(43)Date of publication of application : 28.09.2001

(51)Int.Cl.

G06F 12/14

G06F 3/06

(21)Application number : 2000-244020

(71)Applicant : HITACHI LTD

(22)Date of filing : 07.08.2000

(72)Inventor : ITO RYUSUKE  
OKAMI YOSHINORI

(30)Priority

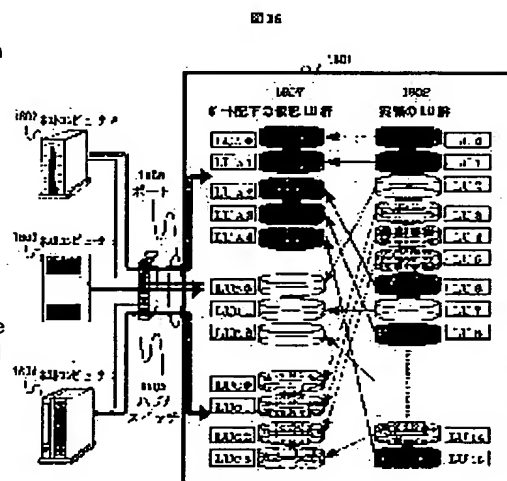
Priority number : 2000010115 Priority date : 14.01.2000 Priority country : JP

## (54) SECURITY SYSTEM FOR STORAGE SUB SYSTEM

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a security function in a storage sub system by the flexible and efficient presentation method of storage resources by performing execution by high-speed judgment logic without affecting a processing on the side of a host computer.

**SOLUTION:** An information WWN for uniquely identifying the host computer, a management table where the correspondence of a logical unit number LUN inside the storage sub system for which access is permitted to the host computer and a virtual LUN for presenting the LUN to be the access object to the host computer by a user optional method is described and the management table where the correspondence of the WWN and a dynamically allocated management number S-ID is described are stored in a nonvolatile memory inside the storage sub system beforehand. By retrieving the WWN of the host computer from the S-ID of the host computer and retrieving the accessible virtual LUN from the WWN, access propriety to the LUN inside the storage sub system is judged.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-265655

(P2001-265655A)

(43) 公開日 平成13年9月28日 (2001.9.28)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード (参考)
G 0 6 F 12/14	3 1 0	G 0 6 F 12/14	3 1 0 J 5 B 0 1 7
3/06	3 0 4	3/06	3 0 4 H 5 B 0 6 5

審査請求 未請求 請求項の数15 O L (全 25 頁)

(21) 出願番号 特願2000-244020 (P2000-244020)

(22) 出願日 平成12年8月7日 (2000.8.7)

(31) 優先権主張番号 特願2000-10115 (P2000-10115)

(32) 優先日 平成12年1月14日 (2000.1.14)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 伊東 隆介

神奈川県小田原市国府津2880番地 株式会

社日立製作所ストレージシステム事業部内

(72) 発明者 岡見 吉規

神奈川県小田原市国府津2880番地 株式会

社日立製作所ストレージシステム事業部内

(74) 代理人 100075096

弁理士 作田 康夫

Fターム (参考) 5B017 AA01 BA02 BB06 CA06 CA16

5B065 BA01 CA30 CA50 PA02 PA04

PA14

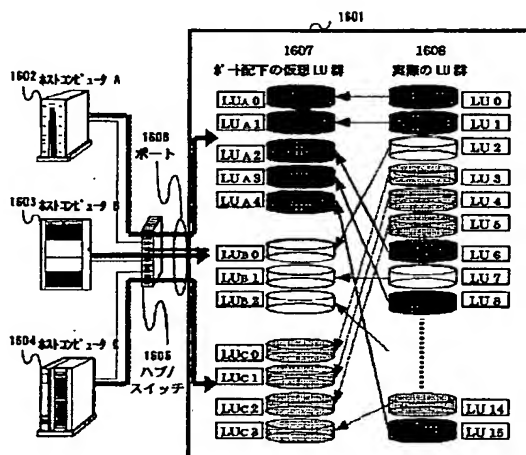
(54) 【発明の名称】 記憶サブシステムのセキュリティシステム

(57) 【要約】

【課題】 記憶サブシステムにおけるセキュリティ機能を、ホストコンピュータ側の処理に影響を与えず高速な判定ロジックで実施し、記憶資源の柔軟で効率的な開示方法により提供すること。

【解決手段】 ホストコンピュータを一意に識別する情報WWNと、このホストコンピュータにアクセス許可した記憶サブシステム内の論理ユニット番号LUNと、このアクセス対象となるLUNをホストコンピュータに対してユーザ任意の方法で開示するための仮想LUNとの対応を記述した管理テーブル、および、WWNと、動的に割り当てられる管理番号S\_IDとの対応を記述した管理テーブル、を予め記憶サブシステム内の不揮発メモリに記憶させ、ホストコンピュータのS\_IDから当該ホストコンピュータのWWNを検索し、更にこのWWNからアクセス可能な仮想LUNを検索することにより、記憶サブシステム内のLUNに対するアクセス可否を判定する。

図 16



## 【特許請求の範囲】

【請求項1】記憶サブシステムであって、記憶領域が1つ以上の論理ユニットに対応している1つ以上の記憶装置と、前記記憶装置へのデータ読み書きを制御する記憶制御装置と、前記論理ユニットを管理するための管理テーブルと、前記管理テーブルを保持するためのメモリを有し、前記管理テーブルは、ホストコンピュータを識別する情報と、ホストコンピュータがアクセス可能な前記論理ユニットを特定する識別番号と、前記論理ユニットの識別番号に対応する仮想的な識別番号の対応を記述しており、前記ホストコンピュータを識別する情報をキーにして前記管理テーブルを参照することにより、ホストコンピュータのアクセス可否が判定できる記憶サブシステム。

【請求項2】請求項1記載の記憶サブシステムであって、前記論理ユニットを特定する識別番号と、前記仮想的な識別番号の対応は、任意に定めることができる記憶サブシステム。

【請求項3】請求項2記載の記憶サブシステムであって、前記論理ユニットを特定する識別番号と、前記仮想的な識別番号の対応において、複数の前記論理ユニット識別番号に、共通の仮想的な識別番号を対応させることができる記憶サブシステム。

【請求項4】保守用端末装置と接続した記憶サブシステムであって、記憶領域が1つ以上の論理ユニットに対応している1つ以上の記憶装置と、前記記憶装置へのデータ読み書きを制御する記憶制御装置と、ホストコンピュータを識別する情報WWN、前記論理ユニットの識別番号LUN、前記LUNに対応する仮想LUNの3者の対応を記述した、前記保守用端末装置により作成した第1の管理テーブルと、前記WWNと、動的に割り当てられる識別番号S\_IDの対応を記述した、前記保守用端末装置により作成した第2の管理テーブルと、前記第1および第2の管理テーブルを保持するためのメモリを有する記憶サブシステム。

【請求項5】請求項4記載の記憶サブシステムであって、前記第1の管理テーブルの対応は、前記WWNと、当該WWNを有するホストコンピュータがアクセス可能な前記LUNと、当該LUNに対応する前記仮想LUNの対応を示すものであり、前記第2の管理テーブルから前記S\_IDをキーに前記WWNを取得し、当該WWNをキーに第1の管理テーブルを検索することにより、特定のS\_IDを有するホストコンピュータの、前記LUNに対するアクセス可否を決定する記憶サブシステム。

【請求項6】請求項5記載の記憶サブシステムであって、前記LUNと前記仮想LUNの対応は、任意に定めることができる記憶サブシステム。

【請求項7】請求項6記載の記憶サブシステムであって、前記LUNと、前記仮想LUNの対応において、複数の前記LUNに、共通の前記仮想LUNを対応させることができる記憶サブシステム。

【請求項8】保守用端末装置と接続した記憶サブシステムであって、記憶領域が1つ以上の論理ユニットに対応している1つ以上の記憶装置と、前記記憶装置へのデータ読み書きを制御する記憶制御装置と、

ホストコンピュータを識別する情報WWNのうち、複数のホストコンピュータに共通な特定の情報、前記論理ユニットの識別番号LUN、前記LUNに対応する仮想LUNの3者の対応を記述した、前記保守用端末装置により作成した第1の管理テーブルと、前記WWNと、動的に割り当てられる識別番号S\_IDの対応を記述した第2の管理テーブルと、前記第1および第2の管理テーブルを保持するためのメモリを有する記憶サブシステム。

【請求項9】請求項8記載の記憶サブシステムであって、前記LUNと前記仮想LUNの対応は、任意に定めることができる記憶サブシステム。

【請求項10】請求項8記載の記憶サブシステムであって、前記複数のホストコンピュータに共通な特定の情報が、ホストのベンダを特定するためのCompany\_IDである記憶サブシステム。

【請求項11】記憶サブシステムであって、記憶領域が1つ以上の論理ユニットに対応している1つ以上の記憶装置と、前記記憶装置へのデータ読み書きを制御する記憶制御装置と、

前記論理ユニットを管理するための管理テーブルと、前記管理テーブルを保持するためのメモリを有し、前記管理テーブルは、ホストコンピュータを識別する情報と、ホストコンピュータが管理する前期論理ユニットの識別番号と、ストレージが管理する前期論理ユニットの識別番号の対応を記述している記憶サブシステム。

【請求項12】請求項11記載の記憶サブシステムであって、前記管理テーブルはホストコンピュータから前記論理ユニットへのアクセス可否の判定に用いられ、前記判定は、前記ホストコンピュータを識別する情報をキーにして前記管理テーブルを参照することにより行われる記憶サブシステム。

【請求項13】請求項11記載の記憶サブシステムであって、同一な論理ユニットに付与されている、前記ホストコンピュータが管理する前期論理ユニットの識別情報と、前記ストレージが管理する前期論理ユニットの識別番号が異なる値を持つことができる記憶サブシステム。

【請求項14】請求項11記載の記憶サブシステムであって、前記ホストコンピュータが管理する前期論理ユニットの識別番号は、任意に付与することができる記憶サブシステム。

【請求項15】請求項11記載の記憶サブシステムであって、前記ホストコンピュータが管理する前期論理ユニットの識別番号は、異なる論理ユニットに同一の値を付与することができる記憶サブシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】ホストコンピュータからアクセスされる記憶サブシステムに関係し、特にホストコンピュータから該記憶サブシステム内の論理ユニットがアクセスされる記憶サブシステムに関する。

【0002】

【従来の技術】これまで、ホストコンピュータから記憶サブシステムへの不正アクセスを防ぐセキュリティ手段として、ホストコンピュータ側のOS (operating system) の機能やミドルウェアもしくはアプリケーション・ソフトウェアを使用する例がよく知られている。

【0003】一方、近年、ファイバチャネル・プロトコルが規格化されたことによって、記憶サブシステムとホストコンピュータとのインタフェースにSCSIや、ESCON、TCP/IPなど様々な既存プロトコルの同時使用が可能となり、記憶サブシステム内の記憶資源が一層有効利用可能となってきた。

【0004】しかし、このような背景においては、複数のホストが1つの記憶サブシステムに対してアクセスしてくるため、従来通りのホスト側のOSやミドルウェア、アプリケーション・ソフトウェアだけでは、記憶サブシステム資源に対するセキュリティ機能として十分ではない、という危惧が発生してきた。このような現状に鑑み、記憶サブシステム資源（論理ユニット）に対するセキュリティ機能の実現手段として、特開平10-333839号公報に開示がある。

【0005】上記公報による方法では、ホストコンピュータが起動する前に、予め記憶サブシステムにアクセスしてくる可能性があるホストコンピュータを一意に識別するN\_Port\_Nameと、アクセスを許可する記憶サブシステム内の論理ユニットの組み合わせを管理したテーブルを記憶サブシステム内に保持する。ホストコンピュータは、起動されると記憶サブシステムに対して、フレームと呼ばれるファイバチャネルプロトコルで規定されたある情報単位によってSCSIコマンドを送信する。記憶サブシステムは、このSCSIコマンドを逐一判定して、その中からアクセス元であるホストコンピュータを規定するN\_Port\_Nameを抽出する。

【0006】抽出されたN\_Port\_Nameは、上

述のN\_Port\_Nameとアクセスを許可した記憶サブシステム内の論理ユニットの組み合わせテーブル上で検索され、そのエントリが存在する場合、当該のホストコンピュータは、当該の論理ユニットへのアクセスを許可され、エントリが存在しない場合、当該ホストコンピュータは、当該の論理ユニットへのアクセスを拒絶される。

【0007】

【発明が解決しようとする課題】記憶サブシステム内の記憶資源（論理ユニット）に対するセキュリティを実現する従来技術は、記憶サブシステムにフレームを送信してくるホストコンピュータに対して、逐一、そのアクセス可否を判定するため、データ転送にしろアクセス可否判定のオーバーヘッドが大きく、高い性能を実現しにくいという課題があった。

【0008】また、従来技術は、記憶サブシステムにフレームを送信してくるホストコンピュータが、そのフレーム内に送信元ホストコンピュータを一意に識別するための情報をもたせる点で、ホストコンピュータ側に新たな機能が必要となっていた。

【0009】更に、従来技術では、アクセスしてくるホストコンピュータに対して、記憶サブシステム内の論理ユニット番号をそのまま開示するため、記憶サブシステムのポート配下にユーザの運用希望にそった論理ユニットの再配列を行えない。更にまた、多くのホストコンピュータでは、起動時に接続されている記憶サブシステムのLU0にアクセスできない場合、そのLU0以降の同系列のLU (SCSI-2の規格では、この1系列は8つのLUで構成されるため、LU0～LU7までが同系列となる。)には全く存在の問い合わせをしない、とするものが多い。

【0010】この場合、サブシステム内の論理ユニット番号をそのまま開示する方法では、アクセスが許可されているにもかかわらず、当該LUNを参照できないという事態が生じる。

【0011】本発明の第1の目的は、ホストコンピュータの既存処理を変更せずに、ホストコンピュータ毎にアクセス可能な論理ユニットを制限し、不正アクセスを防止するセキュリティ機能を、記憶資源の高効率利用と高速なアクセス判定ロジックと共に提供することである。

【0012】本発明の第2の目的は、ホストコンピュータの既存処理を変更せずに、同一ベンダ毎にアクセス可能な論理ユニットを制限し、不正アクセスを防止するセキュリティ機能を、記憶資源の高効率利用と高速なアクセス判定ロジックと共に提供することである。

【0013】また、本発明の第3の目的は、このセキュリティ機能に基づいてアクセスが許可されたベンダのホストコンピュータ群に対して、当該ベンダ向けの記憶資源フォーマットやサービスを提供することである。

【0014】

【課題を解決するための手段】上記課題を解決するために、本発明は以下の記憶サブシステムを提供する。

【0015】ホストコンピュータを一意に識別する情報(WWN)、このホストコンピュータからのアクセスを許可した記憶サブシステム内の論理ユニット番号(LUN)、および該論理ユニット番号に対してユーザが任意のリナンバリング方法で任意数再配列して割り当てた仮想的な論理ユニット番号(仮想LUN)の対応を記述した管理テーブルと、これを格納する不揮発のメモリと、動的に割り当てられる管理番号(S\_ID)(注・「ホストストレージのログイン時に動的に割り当てられる」から変更、以下同じ)、およびホストコンピュータを一意に識別する情報(WWN)の対応を記述した管理テーブルと、これを格納する不揮発のメモリと、1つ以上の記憶装置と、これらの記憶装置に対してデータの読み書きを制御する記憶制御装置と、ホストコンピュータと接続を行うための1つ以上のポートと、前記記憶装置の記憶領域に対応した論理ユニットを有する記憶サブシステム。

【0016】この記憶サブシステムにおいては、ホスト識別情報WWNのかわりに、動的に割り当てられるS\_IDを識別情報として用いるため、I/O処理ごとに、各LUNにアクセス可否を問い合わせる必要がなくなりアクセス時のオーバーヘッドを削減することが可能となる。

【0017】また、仮想LUNを用いることにより、ユーザが任意の方法でLUNの再配列を行うことが可能となる。

【0018】

【発明の実施の形態】本発明では、記憶サブシステムとホストコンピュータ間で使用するインタフェース・プロトコルの例にファイバチャネルを、その上で動作するコマンドセットの例にSCSIコマンドを用いて説明する。しかし本発明の適用は、ファイバチャネルとSCSIコマンドの組み合わせに限定されるものではなく、これらと同様に、ログイン、問い合わせといった機能、機構を提供可能なプロトコルであれば何でもかまわない。

【0019】本発明の第一の実施例を以下に示す。

【0020】ここで、ファイバチャネルは比較的新しいインタフェース・プロトコルであるため、はじめに、そのプロトコルの概要を説明する。

【0021】ファイバチャネルはシリアル転送方式のプロトコルであり、情報を非同期に送るため伝送媒体の帯域幅を有効に利用できる。また、ファイバチャネルは独自のコマンドセットを持たず、従来のSCSI、ESCON、HIPPI、IPI-3、IP等といったコマンドセットのためのインフラとして使用される。これより、従来のプロトコル資産を継承可能であり、かつ、より高速で信頼性の高い多彩なデータ転送を可能とする。

【0022】また、ファイバチャネルはチャネルとネッ

トワークの特長を併せ持つインタフェースである。ファイバチャネルでは一度、転送元と転送先が確定すれば、遅延が少ない高速な転送を実現できるが、これはチャネルの最大の特長の1つである。また、通信を希望する機器は、任意の契機でファイバチャネルの通信系に参加し、通信の目的となる相手の機器と相互に通信に関する取り決め情報を交換し、通信を開始することができるが、これはネットワークの特長である。ここで述べた相手機器との通信に関する取り決め情報交換の手続きを、とくにログインと呼ぶ。

【0023】ファイバチャネルのインタフェースを持つ機器をノードと呼び、実際のインタフェースにあたる物理的な口をポートと呼ぶ。ノードは1つ以上のポートを持つことが可能である。ファイバチャネルの系全体に同時に参加できるポートの数は、最大で24ビットのアドレス数、すなわち約1677万個である。これらの接続を媒介するハードウェアをファブリックと呼ぶ。実際には、送信元および送信先のポートは、ファブリックを意識せずに互いのポートに関する情報のみを考慮して動作すればよい。

【0024】各ノードおよびポートには、標準化団体(IEEE)から一定のルールによって割り当てられる、世界中でユニークな識別子が記憶されている。これは従来からTCP/IPなどで馴染みのMACアドレスに相当するものであり、ハードウェア的に固定なアドレスである。このアドレスにはN\_Port\_Name、Node\_Nameの2種類があり、それぞれ8バイトのサイズを持つ。N\_Port\_Nameはポート毎に固有の値(ハードウェア・アドレス)であり、Node\_Nameはノード毎に固有の値(ハードウェア・アドレス)である。これらは、いずれも世界中でユニークな値であることから、ノードまたは、ポートを一意に識別できるアドレスとして、WWN(World Wide Name)と呼ばれる。本特許の実施例では、WWNと記述した場合、N\_Port\_Nameを指すものとする。

【0025】ファイバチャネルでは、通信はOrdered Setと呼ばれる信号レベルの情報と、フレームと呼ばれる固定のフォーマットを持った論理的な情報とで行われる。図2はフレームの構造を示している。フレーム201は、フレームの始まりを示すSOF(Start of Frame)202と呼ばれる4バイトの識別子、リンク動作の制御やフレームの特徴づけを行う24バイトのフレームヘッダ203、実際に転送される目的となるデータ部分であるデータフィールド204、4バイトの巡回冗長コード(CRC)205、フレームの終わりを示すEOF(End of Frame)206と呼ばれる4バイトの識別子からなる。データフィールド204は0~2112バイトの間で可変である。

【0026】次に、フレームヘッダの内容について説明

する。207はフレームヘッダの構造について示している。ここではフレームヘッダ203の詳細構造207における、1ワード目の0～23ビット領域にあたるS\_ID208についてのみ説明する。S\_ID (Source ID) 208は当該フレームを送信するポートを識別するための3バイトのアドレス識別子であり、送受信されるすべてのフレームで有効な値を持つ。このS\_IDは動的に変動する値であり、ファイバチャネルの規格セットの1つであるFC\_PHでは、S\_IDをファブリックによって、初期化手続き時に割り当てられる、としている。割り当てられる値は、それぞれのポートがもつN\_Port\_Nameまたは、Node\_Nameに依存する。

【0027】次に、ファイバチャネルプロトコルに基づく、送信元の機器と送信先の機器が通信に関して互いに情報を交換するログイン手続きについて述べる。図3に、PLOGIフレームにおけるデータフィールド204の詳細構造について示す。フレーム、およびフレームヘッダの構造は図2と同様である。PLOGIフレームのデータフィールド204において、先頭から21バイト目～29バイト目までの8バイトの領域がN\_Port\_Name307を格納する領域であり、先頭から30バイト目～38バイト目までの8バイトの領域がNode\_Name308を格納する領域である。

【0028】図4は、送信元（ログイン要求元）401と送信先（ログイン受信先）402との間に取り交わされる情報のやりとりを示したものである。ファイバチャネルのログイン手続きには数種類存在するが、ここではクラス3のログインに関して述べる。

【0029】ログイン要求元は、PLOGIフレーム403をログイン受信先へ送信する。このフレームには、ログイン要求元のN\_Port\_Name、Node\_Name、S\_IDおよびその他の情報が含まれている。受信先の装置では、このフレームに含まれている情報を取り出し、ログインを承認する場合は、ACC404と呼ばれるフレームをログイン要求元に対して送信する。一方、ログインを拒絶する場合は、LS\_RJT405と呼ばれるフレームをログイン要求元に対して送信する。

【0030】ログイン要求元は、自らが送信したPLOGIフレームに対してACCフレームの応答を検出すると、ログインが成功したことを知り、データ転送などのI/Oプロセスを開始できる状態となる。一方、ログイン要求元が、LS\_RJTを受信した場合はログインが成立しなかったこととなり、当該ログイン受信先へのI/Oプロセスは実行不可となる。ここではクラス3のログインについて述べたが、他のログインプロセスにおいても、ログイン要求元からログイン受信先へ渡すことのできる情報の中に、N\_Port\_Name、Node\_NameおよびS\_IDが含まれることにおいては同

様である。

【0031】次に、SCSIコマンドセットでは必ずサポートされている標準的なコマンドである、Inquiryコマンドについて説明する。Inquiryコマンドとは、I/Oプロセスを開始するのに先立ち、I/Oプロセスの対象となる論理ユニットに対して、その実装状態、準備状態を問い合わせるコマンドである。

【0032】図5は、SCSI規格で定義されたInquiryコマンドを、ファイバチャネル規格のフレームで送信する場合のデータフィールドの詳細構造を示している。フレーム、およびフレームヘッダの構造は図2と同様であるが、S\_ID208が含まれている。

【0033】データフィールド204には506のFCP\_CMNDフォーマットに示すように、FCP\_LUN 507、FCP\_CNTL508、FCP\_CDB 509、FCP\_DL510と呼ばれる領域がある。ここではFCP\_LUN507、およびFCP\_CDB509について述べる。FCP\_LUN507の中には、フレーム送信元が状態を問い合わせようとする、フレーム送信先のポートに関連付けられた論理ボリューム（目に見える単体としての記憶装置（物理ボリューム）に対して、便宜上仮想的に分割されナンバリングされた記憶領域）の識別子が格納されている。この識別子をLUN (Logical Unit Number) という。FCP\_CDB509の中には、SCSIコマンドセットを使用する場合にはSCSIのコマンド記述ブロック（CDB）と呼ばれる命令情報が格納される。このFCP\_CDB509の中に、SCSIのInquiryコマンド情報が格納されて、前述のFCP\_LUN 507と共に、フレーム受信先へ情報が転送される。

【0034】次に、Inquiryコマンドを受信したフレーム受信先が、問合せへの応答としてフレーム送信元へ返信する情報について述べる。この情報をInquiryデータという。図6にInquiryデータの抜粋を示す。ここでは、Inquiryデータ601のうちクオリファイア602と、デバイス・タイプ・コード603の2つについて述べる。クオリファイア (Peripheral Qualifier) 602は、指定された論理ユニットの現在の状態を設定する3ビットの情報である。論理ユニットの状態604は、このクオリファイアのビットパターンによって示される論理ユニットの状態を示したものである。コード000（2進数）605は、論理ユニットとして接続されている装置は、デバイス・タイプ・コード603の領域に示される種類の入出力機器であることを示している。本コードが設定されていても、その論理ユニットが使用可能、すなわちレディ状態であることを必ずしも示しているわけではない。

【0035】しかし、当該論理ユニットを使用できるのは本コードが設定されている場合に限られる。コード0



01 (2進数) 606は、論理ユニットとして接続されている装置は、デバイス・タイプ・コード603の領域に示される種類の入出力機器であることを示しているが、そのロジカルユニットには実際の入出力機器が接続されていないことを示している。これは例えばCD-ROMドライブが実装されているが、CD-ROM媒体がドライブ内に挿入されていないような場合を示す。

【0036】コード011 (2進数) 607は、指定された論理ユニットがサポートされていないことを示す。従って指定された論理ユニットに装置が割り当てられることはない。本コードが設定されるときは、デバイス・タイプ・コード領域603にはかならず1F (16進数) が設定される。

【0037】デバイス・タイプ・コード (Peripheral Device Type) 603は、指定された論理ユニットに実際に割り当てられている入出力機器の種類を示す5ビットの情報である。コード608は、各デバイスタイプ609に対応する16進数のコードである。608に示されている情報のうち、未定義または未接続のデバイスを表す1F (16進数) 610が設定された場合、Inquiryコマンド送信元が問い合わせたデバイスは未定義あるいは未接続であり、当該論理ユニットは送信元からは使用できない。

【0038】図7に、このInquiryコマンドを用いた論理ユニット問合せの手順を示す。論理ユニットにアクセスしようとするホストコンピュータ701は、アクセスしようとする論理ユニットをもつ記憶サブシステム702に対し、Inquiryコマンドを格納したフレーム703を送信する。

【0039】このフレームには、ホストコンピュータのS\_IDと、問合せを行う先の論理ユニットの識別子であるLUNが含まれている。ここで、LUNについては、FCP\_LUN領域の他に、FCP\_CDB内のInquiryコマンド情報のフォーマット中にも設定することができる。どちらの値を使用しても得られる効果は同じであるが、本実施例ではLUNの値はFCP\_LUN 507に格納された値を使用するものとする。

【0040】Inquiryコマンドを含むフレームを受信した記憶サブシステム702は、問合せに対して必要なInquiryデータを準備し、作成したInquiryデータを含むフレーム704をホストコンピュータに送信する。このときInquiryデータを格納するフレームを、FCP\_DATAと呼ぶ。記憶サブシステムが、問合せのあった論理ユニットについて、クオリファイア000 (2進数)、デバイスタイプ00~09 (16進数) のいずれかを設定する場合704、このInquiryデータを受信したホストコンピュータは、当該論理ユニットに対して、以降I/Oの発行が可能となる。

【0041】一方、705に示すように、記憶サブシ

テムが、クオリファイア001 (2進数) または011 (2進数)、デバイスタイプ1F (16進数) を設定した場合、このInquiryデータ705を受信したホストコンピュータは、当該論理ユニットに対して、以降、I/Oの発行が不可能であることを認識する。

【0042】以上のことから、Inquiryデータに格納するクオリファイア、およびデバイス・タイプ・コードを記憶サブシステム側でコントロールすれば、ホストコンピュータから記憶サブシステムの論理ユニットへのアクセス許可および不許可を制御できることが分かる。

【0043】続いて、本発明の処理の流れについて詳細を述べる。

【0044】はじめに図1は、本発明の実施例の装置構成を示したものである。本装置を記憶サブシステム101とよぶ。記憶サブシステム101は、ファイバチャネル・インタフェース用のポート102~104を有し、ファイバチャネル・インタフェースを介して、ホストコンピュータ105~107と物理的に接続されている。ホストコンピュータ105~107もまた、ファイバチャネルインタフェース用のポート108~112を有しており、ホストコンピュータ105~107と記憶サブシステム101は、ファイバチャネル・プロトコルによる通信が可能である。ホストコンピュータには、105や106のように複数のファイバチャネル・ポートをもつものもあれば、107のように単一のファイバチャネル・ポートしかもたないものもある。

【0045】記憶サブシステム101とホストコンピュータ105~107間のファイバチャネルインタフェースの接続形態 (トポロジ) には、Point-to-Pointや、アービトレーション・ループ接続、ファブリック接続等、いくつかの種類が存在するが、本発明はその接続形態には依存しないため、単にファイバチャネル113と記述する。

【0046】まず、記憶サブシステム101は、種々の演算や処理を行うマイクロプロセッサ114を有し、複数の記憶装置群115、およびこれらにデータの読み書きを制御して行う記憶制御装置116、さらに記憶装置群115と記憶制御装置116を接続するためのバス117を有している。また、記憶サブシステム101は、種々の演算や処理のワーク領域として使用するメモリ118と、種々の管理情報、管理テーブル等を保存しておく不揮発メモリ119を有する。更に、ホストコンピュータへの応答を速くするための工夫として、キャッシュ120を有している。また、記憶サブシステム101は、通信制御部121を有し、通信回線122を介して、保守用端末装置123と接続されている。

【0047】保守用端末装置123は、内部にマイクロプロセッサ124と、ユーザとのインタフェースとなる入力部125と処理の結果を出力する表示部126を有

している。ユーザは、この入力部125を介して、本実施例で定義するいくつかのテーブルの設定を行うことができる。

【0048】図8において、本実施例の処理流れ概要を示す。初めに、手順801において、ユーザは前述の保守用端末装置123の入力部125を介して、記憶サブシステム内に存在するLUを規定するLUN(Logical Unit Number)と、そのLUNにアクセスする可能性のあるホストコンピュータのWWN(N\_Port\_Name)と、これにアクセスしてくるホストコンピュータに対してそのLUNをどのように見せるかを決定する仮想LUNとを結び付けた「LUNアクセス管理テーブル」を作成する。

【0049】本テーブルは、記憶サブシステム内の不揮発メモリ119に保持される。各ホストコンピュータには、本テーブルの仮想LUNが見える。各ホストコンピュータのWWNは既知である。

【0050】手順802において、各ホストコンピュータが記憶サブシステムに対して、ファイバチャネル・プロトコルに基づいてログインしてくると、記憶サブシステムはPLOGIフレームから、当該ホストコンピュータのWWNと、S\_IDを切り出し、それらの組み合わせを記述した「WWN-S\_ID変換テーブル」を作成し、不揮発メモリ119上にこれを保持する。記憶サブシステムはこの作業を全てのPLOGIフレームに対して行う。

【0051】次に手順803において、記憶サブシステムは、各ホストコンピュータが記憶サブシステム内の論理ユニットの状態を知るために送信したInquiryコマンドを含むフレームを受信する。このフレームを受信した記憶サブシステムは、そのフレームのヘッダからS\_IDを、データフィールドからInquiryコマンドの対象となるLUNを切り出す。続いて、記憶サブシステムは、このS\_IDをキーにして上述の「WWN-S\_ID変換テーブル」を検索し、このS\_IDに相当するWWNを取得する。

【0052】続いて、記憶サブシステムは、手順804において、得られたWWNをキーにして上述の「LUNアクセス管理テーブル」を検索し、Inquiryコマンドの対象となっているLUNに相当する仮想LUNを「LUNアクセス管理テーブル」から取得する。ここでInquiry対象となっているLUNを仮想LUNとして取得する理由は、ホストコンピュータには仮想LUNが開示されているためである。

【0053】続いて手順805では、手順804の結果、当該WWNに対応する仮想LUNを取得できたか否かの判定を行う。取得できた場合、すなわち当該WWNに対応する仮想LUNが「LUNアクセス管理テーブル」上に存在した場合は、当該ホストコンピュータによる当該仮想LUNへのアクセスが許可される。対応する

仮想LUNが該テーブルに存在しない場合は、当該ホストコンピュータにより当該仮想LUNへのアクセスが拒絶される。

【0054】手順805の結果、当該ホストコンピュータによる当該仮想LUNへのアクセスが許可される場合、記憶サブシステムは、手順806において、ホストコンピュータの発行したInquiryコマンドに対して、対象LUが実装済みの設定(すなわちアクセス可能である旨の設定)を行った上で、Inquiryデータを送信する。

【0055】一方、当該仮想LUへのアクセスが拒絶される場合、記憶サブシステムは、手順807によって、ホストコンピュータの発行したInquiryコマンドに対して、対象LUが未実装の設定(すなわちアクセス不可である旨の設定)を行った上で、Inquiryデータを送信する。

【0056】Inquiryデータを受信したホストコンピュータは、そのフレームを解析する。

【0057】解析の結果、記憶サブシステムの当該仮想LUNへのアクセス許可を認識すると、ホストコンピュータは以降、当該仮想LUNに対して、コマンド(I/O要求)を継続して発行することができる。この場合、手順808にあるように、記憶サブシステムは当該ホストコンピュータからのログインが有効である間は、当該LUへのアクセス可否をチェックしなおすことなく、コマンド受信を継続することができる。

【0058】一方、当該LUNへのアクセス拒否を認識したホストコンピュータは、記憶サブシステムへのログインが有効である間、当該LUへ再度アクセスすることはない。

【0059】以下、上記の記憶サブシステム内の特定LUNに対するホストコンピュータからのアクセス可否を制御する方式を、便宜的に「LUNセキュリティ」と呼ぶ。

【0060】次に、上記の各手順について詳細を示す。

【0061】はじめに、上記手順の「LUNアクセス管理テーブル」の作成について記述する。本発明におけるLUNセキュリティは、記憶サブシステムのもつポート毎に管理されるものとし、ホストコンピュータは、この記憶サブシステムのポートを通して、記憶サブシステム内のLUにアクセスするものとする。この場合、最も簡単な方法として、ホストコンピュータを一意に識別する情報であるWWNと、当該ホストコンピュータにアクセスを許可するLUN(Logical Unit Number)の対応を定義した、図9に示すようなテーブル901を、記憶サブシステム内に設ければよい。

【0062】しかし、ホストコンピュータと記憶サブシステム間に、ファイバチャネル対応のハブや、スイッチなどの機器類が存在するような使用環境では、901のテーブルだけでは不十分である。以下それを説明する。

【0063】テーブル901は、記憶サブシステム内のLUをその識別子であるLUN (Logical Unit Number) に基づき、そのままホストコンピュータのWWNに対して割り当てている。図9では、WWN902のホストコンピュータには、LU0～2にのみアクセスが許可され、WWN903のホストコンピュータは、LU3、4、および7にのみアクセスが許可され、WWN904のホストコンピュータは、LU5～6にのみアクセスが許可されている。

【0064】したがって、例えばLU0～2は、WWN902のホストコンピュータ以外のホストコンピュータからは、アクセス不可となり、LUNセキュリティが実現される。しかし、今日多くのホストコンピュータでは、起動時に接続されている記憶サブシステムのLU0にアクセスできない場合、そのLU0以降の同系列のLU (SCSI-2の規格では、この1系列は8つのLUで構成されるため、LU0～LU7までが同系列となる。) には全く存在の問い合わせをしない、とするものが多い。

【0065】すると、テーブル901のような規定方法では、ホストコンピュータ903や904は、アクセス許可するLUNがそれぞれ規定されていないが、LU0にアクセスできないために、テーブル901で規定したアクセス許可のLUNを参照できない事態が発生してしまう。このような現象は、ディスクアレイ装置のような記憶資源を豊富に提供し得る装置においては、著しくその利用率を下げってしまうことになり無駄である。

【0066】そこで、これを防ぐためにホストコンピュータ903、904にLU0へのアクセスを許可すると、LU0のセキュリティが保証されない。仮にこれを認めた場合にも、ホストコンピュータ903と904が異なるOSをもつホストコンピュータである場合、LU0を共有することは、それぞれのOSによるフォーマットの違いなどから困難である。

【0067】一方、図10においてホストコンピュータが接続している当該ポート配下にLU0が存在しなくても、全てのLUNに対して存在の問い合わせを行う、WWN1002～1004を持つホストコンピュータ群が存在すると仮定する。ここでは、WWN1002のホストコンピュータは、LU0、1、7にのみアクセスが許可され、WWN1003のホストコンピュータは、LU3、5、6にのみアクセスが許可され、WWN1004のホストコンピュータは、LU2、4にのみアクセスが許可されている。

【0068】この状態を視覚的に表したのが図11である。ホストコンピュータ1102～1104は、図10 WWN1002～1004を持つホストコンピュータに相当する。ホストコンピュータ1102～1104は、ファイバチャネル対応のハブや、スイッチ1105を経由して記憶サブシステムの同一のポート1106に接続

している。このような使用環境において、各々のホストコンピュータ1102～1104に対し、無計画にアクセス対象LUNを定義したり、以前割り当てたLUNと異なるLUNをアクセス対象として割り当てた場合、ホストコンピュータに記憶サブシステム内のLUNをそのまま開示している1101のような記憶サブシステムではLUNの開示方法に柔軟性がないため、当該ポート配下が、LU群1107のようにLUが離散した状態で見え、使用上、著しく管理しにくい状態となってしまう。

【0069】一方、最近、記憶サブシステムの1つのポート配下に9個以上のLUを定義しても、これを認識するホストコンピュータが存在するが、このようなホストコンピュータと従来のように1つの記憶サブシステムのポート配下にLU0～7までの8個のLUしかサポートしないホストコンピュータ間でLUNセキュリティを実施した場合の問題点を示す。

【0070】図12において、WWN1202、1204を持つホストコンピュータが、接続する記憶サブシステムのポート配下にLU0が存在しなくても、各LUに存在の問い合わせを行う機構をもち、かつ、接続する記憶サブシステムのポート配下にLUを16個まで認識する場合について以下説明する。

【0071】WWN1203を持つホストコンピュータは、接続する記憶サブシステムのポート配下にLU0が存在しなくても、各LUに存在の問い合わせを行えるが、サポート可能なLUはLU0～7の範囲の8個までとする。テーブル1201から分かるように、WWN1202を持つホストコンピュータはLU0～5の範囲でアクセスが許可されており、WWN1203を持つホストコンピュータはLU6～10の範囲で、またWWN1204を持つホストコンピュータはLU11～15の範囲でアクセスが許されている。この状態を視覚的に表したのが図13である。

【0072】ホストコンピュータ1302～1304は、図12のWWN1202～1204を持つホストコンピュータに相当する。ホストコンピュータ1302～1304は、ファイバチャネル対応のハブや、スイッチ1305を経由して記憶サブシステムの同一のポート1306に接続している。このような使用環境において、各々のホストコンピュータ1302～1304に対して、LU群1308のように記憶サブシステム内のLUを割り当てたとすると、ホストコンピュータA1302には、LU群1308中のLU0～5の範囲のみアクセス許可対象として見え、ホストコンピュータC1304には、LU群1308中のLU11～15の範囲のみアクセス許可対象として見え、それぞれLUNセキュリティの目的を果たすことができる。しかし、ホストコンピュータB1303は、元々1ポート配下にLU0～7までの範囲で、8個までしかLUをサポートできないため、LU群1307の範囲内でしか問い合わせを実施す

ることができない。よって、テーブル1201において、LU6～10までアクセス許可をしても、実際には、LU6、7にしかアクセスできないという問題が生じる。これも、記憶サブシステム内のLUをそのまま開示しているために起こる弊害である。

【0073】以上のような懸念を考慮して、本発明では、図14に示すような「LUNアクセス管理テーブル」1401を定義する。テーブル1401は、図9のテーブル901、図10のテーブル1001、図12のテーブル1201のように記憶サブシステム内のLUNをWWNに直接割り当てたテーブルとは異なり、記憶サブシステム内のLUNと、そのLUNをユーザの任意のリナンバリング方法で定義しなおした仮想LUNと、その仮想LUNにアクセスする可能性のあるホストコンピュータのWWNを組み合わせて記憶サブシステムのポート毎に定義したテーブルである。

【0074】このテーブル1401において、ユーザは任意個数の任意LUNに対して、任意のリナンバリング方法で仮想LUNを対応づけることができる。その結果、この「LUNアクセス管理テーブル」1401を定義した記憶サブシステムでは、各ホストコンピュータに対して、ユーザの任意の使用希望に沿った形でLUNを開示することができる。その際、各ホストコンピュータにアクセスが許可されるLUNは、実際のLUN1417ではなく、仮想LUN1416であるため、各ホストコンピュータに記憶サブシステム内のLUNのばらつきや、LU0の有無などを意識させる必要がなく、ユーザの意志によって最適化された柔軟なLUN状態を提供することができる。

【0075】図14において、WWN1402を持つホストコンピュータは、仮想LUN0～3を通して、実際のLUN0～3へアクセスが許可されている。以下WWN1403～1414を持つホストコンピュータも同様であり、それぞれ仮想LUN1416を通して、対応する実際のLUN1417へアクセス許可される。これにより、各ホストコンピュータは、非LU0に対しても、LU0に対して行うような処理を実行すること等が可能となる。

【0076】この「LUNアクセス管理テーブル」1401において特徴的なことは、WWN1402～1405を持つホストコンピュータには、それぞれ接続ポート配下のLU0にアクセスしているように見えているものの、実際には、それぞれの間で排他的なセキュリティが実現されながら、実際には異なったLUNにアクセスし、記憶資源を効率的に使用できていることである。実際のLUNに対する仮想LUNのリナンバリングに関して詳細を示す。使用者が最もよく行うと思われる仮想LUNによるリナンバリング方法は、従来のSCSI規格との対応を意識して、各WWNに対して、LU0を起点に1ずつLUNが増えていくような番号付け、すなわち

WWN1402～1404の欄に見られるようなケースである。

【0077】しかし、運用面を考慮して、WWN1407、1408の欄のように、偶数のみの仮想LUN、奇数のみの仮想LUNを対応させることも可能である。この例では、WWN1407、1408を有するホストコンピュータがアクセス許可されているのは、実際には単に連続するLU30～34、およびLU35～38である。また、WWN1409の欄のように、LU0が存在しなくても任意のLUNを検出できるようなホストコンピュータに対しては、アクセス希望するLUNに対応する仮想LUNにだけアクセス許可すればよい。また、WWN1410および1411の欄のような対応づけは、2つ以上の異なるホストコンピュータを任意にグルーピングする際に便利である。さらにまた、WWN1412および1413の欄は、これら2つのWWNを有するホストコンピュータに対しては、異なるLUNにアクセス許可しているように見せながら、実際には全く同じLUNにアクセスさせ、同一の情報を開示したい場合に便利な運用である。

【0078】さらには、記憶サブシステムがRAIDを構成するディスクアレイ装置であるような場合に、異なるRAIDグループに属するLUをひとつずつ割り当て、最もI/Oに貢献する記憶装置（磁気ディスクドライブ）数が多くなるようにすることもできる。図14の例でいうと、WWN1414の欄がこれに該当する。

【0079】以上、本発明の「LUNアクセス管理テーブル」による仮想LUNと実際のLUN対応づけの効果について具体例に説明してきたが、これを視覚的に表すと図16のようになる。対応する管理テーブル1502は図15に示した。

【0080】テーブル1501で、各ホストコンピュータに割り当てた実際のLU群1504は、実際には図16の1608のように全く乱雑な配置をとっている。しかし、これをテーブル1501の仮想LU群1503で置換することで、各ホストコンピュータに記憶サブシステム1601内の実際のLUの配置状態1608に影響を受けない状態1607でLUを開示することができる。これにより、記憶サブシステム資源の柔軟な運用が可能となる。

【0081】本発明の「LUNアクセス管理テーブル」1401や1501は、図17手順1701～1703に示すように、記憶サブシステムの全ポートに対して定義された後、記憶サブシステム内の不揮発メモリに保持される。不揮発メモリに保持されることで、本テーブルは、記憶サブシステムの電源切断によっても消失しない。

【0082】続いて、記憶サブシステムがホストコンピュータから、ログインされる際の処理について説明する。本実施例では、一連のログイン処理を通じて、ホス

トコンピュータを一意に識別するWWNと、ログイン以降に使用されるホストコンピュータを一意に識別するS\_IDとを対応させる。ホストコンピュータが起動すると、図18の手順1801において、記憶サブシステムは、PLOGIフレームを受信する。

【0083】PLOGIフレームを受信した記憶サブシステムは、手順1802において、フレームヘッダからホストコンピュータのS\_IDを、手順1803において、データフィールドからホストコンピュータのWWN(N\_Port\_Name)を取得する。続いて、記憶サブシステムは手順1804において、このWWNとS\_IDの組み合わせを図19に示す「WWN-S\_ID変換テーブル」1901に記録作成し、これを手順1805において、記憶サブシステム内の不揮発メモリに保持する。「WWN-S\_ID変換テーブル」1901は、記憶サブシステムのポート毎に作成される。

【0084】このテーブルに登録されたWWNをもつホストコンピュータから、以後、コマンドが送信されると、記憶サブシステムはそのフレームヘッダからS\_IDを取得し、「WWN-S\_ID変換テーブル」1901によってそのホストコンピュータのWWNを検索することができる。記憶サブシステムは、この「WWN-S\_ID変換テーブル」を不揮発メモリ上に保存すると、手順1806において、当該ホストコンピュータのログインを承認した旨のACCフレームを送信する。記憶サブシステムからACCフレームを受信したホストコンピュータは、これ以降、記憶サブシステムに対してInquiryコマンドを発行することができる。

【0085】続いて、ホストコンピュータからのInquiryコマンド受信と、これに対する記憶サブシステムのセキュリティ応答について説明する。図20、図21は、この一連の処理の流れを示したものであり、図22は、この一連の処理の流れにおいて使用される各テーブルやパラメータの参照関係を示したものである。図20の手順2001において、記憶サブシステムは、ホストコンピュータからファイバチャネルに規定されたFCP\_CMNDフレームを受信する。すると記憶サブシステムは、手順2002において、そのFCP\_CMNDのデータフレームの内容を解析する。

【0086】続いて記憶サブシステムは、手順2003において、当該のFCP\_CMNDの内容がInquiryコマンドであるか否かをチェックする。Inquiryコマンドでない場合、記憶サブシステムは手順2004において、そのコマンドに対応した処理を実行する。一方、Inquiryコマンドであった場合、記憶サブシステムは手順2005において、当該FCP\_CMNDフレームのヘッダからホストコンピュータのS\_IDを取得し、手順2006において、当該FCP\_CMNDフレームのデータフィールドのFCP\_LUNから対象とするLUNを取得する。引き続き、記憶サブシ

ステムは手順2007において、得られたS\_IDをキーにして、図19の「WWN-S\_ID変換テーブル」1901を検索し、このS\_IDに対応するWWNを取得する。ここまでの流れは、図22の2201および手順2202、2203の参照動作を指す。

【0087】続いて、手順2008において、このWWNに対してアクセス許可されている仮想LUN情報を取得する。そして、手順2109において、このWWNをもつホストコンピュータのInquiryコマンドから得られたLUNが、「LUNアクセス管理テーブル」上でアクセス許可された仮想LUNとして登録されているか否かを判定する。ここまでの流れは、図22の手順2204および2205の参照動作を指す。

【0088】「LUNアクセス管理テーブル」の当該エントリに、手順2006で得られたLUNが仮想LUNとして登録されている場合、当該ホストコンピュータからその仮想LUNへのアクセスが許可されるため、記憶サブシステムは手順2110において、ホストコンピュータ応答用Inquiryデータのクオリファイアに2進数の'000'を、デバイスタイプに記憶サブシステムのデバイスタイプコードをセットする。

【0089】一方、「LUNアクセス管理テーブル」の当該エントリに、手順2006で得られたLUNが仮想LUNとして登録されていない場合、当該ホストコンピュータからその仮想LUNへのアクセスは拒絶されるため、記憶サブシステムは手順2111において、ホストコンピュータ応答用Inquiryデータのクオリファイアに2進数の'001'または、'011'を、デバイスタイプに16進数の'1F'をセットする。

【0090】次に記憶サブシステムは、手順2112において、FCP\_DATAフレームに上記の応答用Inquiryデータをセットして、ホストコンピュータへ送信する。続いて記憶サブシステムは、手順2113において、ホストコンピュータのInquiryコマンドの応答を完了したことを示すFCP\_RSPフレームを送信する。

【0091】図20の手順2110、2112に引き続いて、Inquiryデータを含むFCP\_DATAを記憶サブシステムから受信したホストコンピュータは、当該LUNへのアクセスは可能と判断し、以降、当該仮想LUNへのアクセス可否を再度問い合わせることなく、アクセスを継続することができる。ここで、当該ホストコンピュータがアクセスするLUNは、実際には図22の手順2206の参照動作でポイントされる、仮想LUNと一意に対応づけられた記憶サブシステム内のLUNとなる。この手順2206の参照動作は、記憶サブシステムの内部的な参照作業であり、ホストコンピュータから意識されることはない。一方、手順2111、2112に引き続いて、Inquiryデータを含むFCP\_DATAを記憶サブシステムから受信したホストコ

ンピュータは、当該LUNへのアクセスは不可能と判断し、以降、当該LUNへのアクセス可否を再度問い合わせることはなく、当該仮想LUNへもアクセスしない。

【0092】本実施例では、上記したようにホストコンピュータがアクセス可否を当該LUNへ問い合わせるのは、Inquiryコマンド発行時だけである。つまり、ログインが有効である間は、この問い合わせを繰り返し行う必要がない。これにより、ホストコンピュータと記憶サブシステム間のデータ転送効率を落とすことなく、強固なLUNセキュリティを実現できる。

【0093】以上のように、記憶サブシステム内に存在するLUNと、そのLUNをユーザ任意のリナンバリング方法で定義しなおした仮想LUNと、その仮想LUNにアクセスする可能性のあるホストコンピュータのWWNとを組み合わせて記憶サブシステムのポート毎に管理することにより、ホストコンピュータ側の処理を変えことなく、記憶サブシステム内の記憶資源を有効に提供でき、当該ホストコンピュータから当該LUNへのアクセス可否を高速な判定ロジックで行う強固なLUNセキュリティを実現できる。

【0094】本実施例では、ファイバチャネルを例に説明したが、実施においては、必ずしもファイバチャネルに限定する必要はなく、同等機能を提供可能なプロトコル環境であれば、その種別は問わない。また、記憶サブシステムに関しても、本実施例では、主にディスクアレイ装置を想定して記述しているが、記憶装置を可換媒体として置き換え、光ディスクライブラリや、テープライブラリなどに適用することも可能である。

【0095】本発明に係る第二の実施形態を以下に説明する。

【0096】第二の実施例も第一の実施例同様、ホストコンピュータと記憶サブシステム間のインタフェース・プロトコルにファイバチャネルを例にして説明する。本実施例は、複数のホストコンピュータから構成される特定のグループに対してLUNセキュリティを実現する方法である。

【0097】例えば、ホストコンピュータと記憶サブシステム間にファイバチャネル対応のハブや、スイッチなどの機器類が存在する図1、図11、図13、図16のような使用環境では、記憶サブシステムの同一ポートにアクセスするホストコンピュータには様々なベンダ製のものが予想される。このような様々なベンダ製のホストコンピュータが共存するような環境では、しばしば記憶サブシステム内の記憶資源の共有、共用に関して問題が発生する。ベンダが異なれば、多くの場合、当該ホストコンピュータの搭載するOSが異なる。この問題は、ホストコンピュータが、WSやメインフレーム等の場合にしばしば発生する。ホストコンピュータがPCの場合は、ベンダが異なっても、OSは多くの場合Windows（登録商標）系であるためこの限りではない。

【0098】OSが異なる場合、記憶資源に対するフォーマット形式や、アクセスのロジック、実行可能なスクリプト、アプリケーション等が異なるため異なるベンダ製ホストコンピュータ間で同一のボリュームを共有することは困難である。

【0099】そこで、記憶サブシステムの記憶資源に対して、ベンダ単位でグルーピングしてアクセスの可否を設定できるような、いわゆるベンダ毎のLUNセキュリティ機能を実現することが望ましい。更に、このようなベンダ毎のLUNセキュリティが実現できれば、アクセスを許可したグループ向けの記憶資源上に、当該ベンダ向けのサービスを提供したり、固有の処理を実行させることもできる。

【0100】そこで、記憶サブシステム内のLUNへアクセスを許可する最小単位をホストコンピュータのベンダ単位で規定することを例に、第二の実施例を説明する。第二の実施例が第一の実施例と異なる点は、「LUNアクセス管理テーブル」の定義方法である。本実施例では、WWNの性質に注目してホストコンピュータのベンダを識別する。図23の2301は、WWNのフォーマットの1つを示したものである。この図から分かるように、WWN2301は、60～63ビットエリア（4ビットエリア）に定義された識別フィールド2302と、36～59ビット（24ビットエリア）に定義されたCompany\_ID2303と、0～35ビット（36ビットエリア）に定義されたVSI D (Vendor Specific Identifier) 2304から構成される。

【0101】このCompany\_ID2303は、従来からよく知られているMACアドレスを原則的に流用したもので、IEEEが世界中のコンピュータベンダや、通信機器ベンダ等を対象にユニークに割り当てた識別情報である。VSI D2304は、IEEEからCompany\_ID2303の使用を認められたベンダが自社のルールで決定したユニークな識別情報であり、当該ベンダ内でユニークな値となる。各ベンダのCompany\_ID2303は、IEEEの出版物等を通して誰でも知ることができる情報であることから、このCompany\_ID2303を予め調べておけば、記憶サブシステムにログインしてきたホストコンピュータがどのベンダ製のものであるかを識別することができる。

【0102】WWNには、何種類かのフォーマット形式が規定されているが、Company\_ID2303とVSI D (Vendor Specific Identifier) 2304を共通して内包している。

【0103】図24は、本実施例における「LUNアクセス管理テーブル」2401である。「LUNアクセス管理テーブル」2401は、記憶サブシステム内のLUN2304と、そのLUNをユーザの任意のリナンバリング方法で定義しなおした仮想LUN2403と、その

仮想LUNにアクセスする可能性のあるホストコンピュータのベンダを表すCompany\_ID 2402を組み合わせて記憶サブシステムのポート毎に定義したテーブルである。このテーブル2401においてユーザは、任意個数の任意LUNに対して、任意のリナンバリング方法で仮想LUNを対応づけることができる。

【0104】その結果、この「LUNアクセス管理テーブル」2401を定義した記憶サブシステムでは、各ベンダ製のホストコンピュータに対して、ユーザの任意の使用希望に沿った形でLUNを開示することができる。その際、各ベンダのホストコンピュータにアクセスが許可されるLUNは、実際のLUN 2404ではなく、仮想LUN 2403であるため、各ベンダ製のホストコンピュータに記憶サブシステム内のLUNのばらつきや、LUNの有無などを意識させる必要がなく、ユーザの意志によって最適化されたLUN状態を提供することができる。

【0105】一方、「WWN-S\_ID変換テーブル」に関しては、本発明の第一の実施例図18に示したものと同様の作成方法で、図19の1901と同様のフォーマットで実現することができる。

【0106】続いて、図25において、本実施例の全体の処理流れを示し、同時に図26において、この一連の処理の流れにおいて使用される各テーブルとパラメタの参照関係を示す。初めに、手順2501において、ユーザは前述の保守用端末装置123の入力部125を介して、記憶サブシステム内に存在するLUNと、そのLUNにアクセスする可能性のあるホストコンピュータ群のベンダを表すCompany\_IDと、これにアクセスしてくる各ベンダ製ホストコンピュータに対してそのLUNをどのように見せるかを決定する仮想LUNとを結び付けた「LUNアクセス管理テーブル」を作成する。

【0107】本テーブルは、記憶サブシステム内の不揮発メモリ119に保持される。各ベンダ製ホストコンピュータには、本テーブルの実際のLUNではなく、仮想LUNが見える。Company\_IDは各ベンダを表す既知の情報である。本実施例の「LUNアクセス管理テーブル」において、WWNではなくWWNの構成要素であるCompany\_IDを使用するのは、LUへのアクセス可否判定を個々のホストコンピュータ単位ではなく、各ベンダ単位で行うためである。

【0108】手順2502において、各ホストコンピュータが記憶サブシステムに対して、ファイバチャネル・プロトコルに基づいてログインしてくると、記憶サブシステムはPLOGIフレームから、当該ホストコンピュータのN\_Port\_Name（以下、これをWWNと記す）と、S\_IDを切り出し、それらの組み合わせを記述した「WWN-S\_ID変換テーブル」を作成し、不揮発メモリ119上にこれを保持する。記憶サブシス

テムは、この作業を全てのPLOGIフレームに対して行う。

【0109】次に手順2503において、記憶サブシステムは、各ベンダ製ホストコンピュータが記憶サブシステム内の論理ユニットの状態を知るために送信したInquiryコマンドを含むフレームを受信する。このフレームを受信した記憶サブシステムは、そのフレームのヘッダからS\_IDを、データフィールドからInquiryコマンドの対象となるLUNを切り出す。続いて、記憶サブシステムは、このS\_IDをキーにして上述の「WWN-S\_ID変換テーブル」を検索し、このS\_IDに相当するWWNを取得する。

【0110】続いて記憶サブシステムは、手順2504において、得られたWWNから、図23の2301のフォーマットに基づいて、24ビットのCompany\_IDを切り出す。このCompany\_IDの切り出し作業は、第一の実施例の流れにはなかった本実施例に固有のものである。手順2503、2504は図26の2601～2604に相当する。

【0111】次に記憶サブシステムは、得られたCompany\_IDをキーにして上述の「LUNアクセス管理テーブル」を検索し、Inquiryコマンドの対象となっているLUNに相当する仮想LUNを「LUNアクセス管理テーブル」から取得する。ここで、Inquiry対象となっているLUNを仮想LUNとして取得する理由は、仮想LUNが記憶サブシステムのLUNとして各ベンダ製ホストコンピュータに対して開示されているためである。

【0112】続いて手順2506では、手順2505の結果、当該WWNに対応する仮想LUNを取得できたか否かの判定を行う。取得できた場合、すなわち当該WWNに対応する仮想LUNが「LUNアクセス管理テーブル」上に存在した場合が、当該ベンダ製ホストコンピュータに対して当該仮想LUNへのアクセスが許可される場合であり、存在しない場合が、当該ベンダ製ホストコンピュータに対して当該仮想LUNへのアクセスが拒絶される場合である。

【0113】手順2506の結果、当該ベンダ製ホストコンピュータによる当該仮想LUNへのアクセスが許可できる場合、記憶サブシステムは、手順2507において、当該ベンダ製ホストコンピュータの発行したInquiryコマンドに対して、対象LUが実装済みの設定、すなわちアクセス可能である旨の設定を行った上で、Inquiryデータを送信する。これら手順2505、2506、2507は図26の2605、2606、2608に相当する。

【0114】一方、手順2506の結果、当該ホストコンピュータにより当該仮想LUNへのアクセスが拒絶される場合、記憶サブシステムは、手順2508によって、当該ベンダ製ホストコンピュータの発行したInq



u i r yコマンドに対して、対象LUが未実装の設定、すなわちアクセス不可である旨の設定を行った上で、I n q u i r yデータを送信する。I n q u i r yデータを受信したホストコンピュータは、そのフレームを解析する。

【0115】解析の結果、記憶サブシステムの当該仮想LUNへのアクセス許可を認識すると、当該ベンダ製ホストコンピュータは以降、当該仮想LUNに対して、コマンド（I/O要求）を継続して発行することができる。この場合、手順2509にあるように、記憶サブシステムは当該ベンダ製ホストコンピュータからのログインが有効である間、当該LUNへのアクセス可否をチェックしなおすことなく、コマンド受信を継続することができる。ここで、当該ベンダ製ホストコンピュータのアクセスが許可されるLUNは、実際には図26の手順2607の参照動作でポイントされる、仮想LUNと一意に対応づけられた記憶サブシステム内のLUNとなる。この手順2607の参照動作は、記憶サブシステムの内部的な参照作業であり、ホストコンピュータから意識されることはない。

【0116】一方、記憶サブシステムが送信したI n q u i r yデータフレームから、当該LUへのアクセス拒否を認識した各ベンダ製ホストコンピュータは、記憶サブシステムへのログインが有効である間、当該LUNへ再度アクセスすることはない。

【0117】本実施例では記憶サブシステムにアクセスしてきたホストコンピュータのWWNを直接セキュリティの管理対象としているのではなく、WWNを構成する情報であるCompany\_IDを切り出して、当該ホストコンピュータが属するグループ、すなわちベンダを規定し、セキュリティの管理対象単位としていることが分かる。

【0118】このことをより詳細に説明しているのが図27と図28である。2701の「LUNアクセス管理テーブル」では、Company\_ID0000E1をもつベンダ製ホストコンピュータ群2705に対して、仮想LUN0、1、2、3、4を通して、実際のLUN0、1、6、8、15へのアクセスを許可している。同様に、Company\_ID0000E2をもつベンダ製ホストコンピュータ群2706に対して、仮想LUN0、1、2を通して、実際のLUN2、7、10へのアクセスを、Company\_ID0000F0をもつベンダ製ホストコンピュータ群2707に対しては、仮想LUN0、1、2、3を通して、実際のLUN3、4、5、14へのアクセスを許可している。

【0119】これを図示したのが図28である。種々のコンピュータ2803～2811は、ファイバチャネルのファブリック2802を経由して、記憶サブシステム2801に単一のポートで接続している。ホストコンピュータ2803～2811は、それぞれ世界でユニーク

なWWNを有しているが、同じベンダ製のホストコンピュータは共通のCompany\_IDを有している。ホストコンピュータ2803、2804、2805、2808が同一のベンダA製であり、そのCompany\_IDは、0000E1とすると、これらのホストコンピュータは、所属するファイバチャネルのドメインが異なっても、2701の「LUNアクセス管理テーブル」のセキュリティ規定から、記憶サブシステム2801内のLUA0～4にのみアクセスが許可される。

【0120】同様にホストコンピュータ2806、2807、2811が同一のベンダB製であり、そのCompany\_IDは、0000E2とすると、これらのホストコンピュータは、所属するファイバチャネルのドメインが異なっても、2701のテーブルのセキュリティ規定から、記憶サブシステム2801内のLUB0～2にのみアクセスが許可される。同様にホストコンピュータ2809、2810が同一のベンダC製であり、そのCompany\_IDは、0000F0とすると、これらのホストコンピュータは、所属するファイバチャネルのドメインが異なっても、2701のテーブルのセキュリティ規定から、記憶サブシステム2801内のLUC0～3にのみアクセスが許可される。これら異なるベンダ間では、2701のテーブルのセキュリティ規定に基づいたアクセスの排他論理により、異なるベンダ用にアクセス制限されたLUを見ることはできない。以上のように、ベンダ毎のLUNセキュリティを実現することができるが、これを応用することで、更にベンダ毎のホストコンピュータ群に記憶サブシステム資源を有効に提供することができる。例えば、2812のLUA0～4、LUB0～2、LUC0～3は、それぞれアクセスしてくるベンダが異なることが自明であるため、それぞれに対して、アクセス許可したベンダ製ホストコンピュータOS向けのフォーマットを実施することができる。また、それぞれに、アクセス許可したベンダ製ホストコンピュータOS向けの固有の実行スクリプトや、アプリケーション・ソフトウェア、サービスを提供することも可能である。更には、それぞれに記憶サブシステム2801の制御情報を提供することで、ベンダ毎に当該記憶サブシステム2801をカスタマイズさせることも可能である。

【0121】以上のように、記憶サブシステム内に存在するLUと、そのLUをユーザの任意のリナンバリング方法で定義しなおした仮想LUNと、その仮想LUNにアクセスする可能性のあるコンピュータベンダのCompany\_IDを組み合わせて記憶サブシステムのポート毎に管理することにより、ホストコンピュータ側の処理を変えることなく、記憶サブシステム内の記憶資源を有効に提供でき、当該ホストコンピュータから当該LUNへのアクセス可否をベンダ単位で高速な判定ロジックで行う強固なLUNセキュリティを実現することがで



きる。

【0122】本実施例では、ファイバチャネルを例に説明したが、実施においては、必ずしもファイバチャネルに限定する必要はなく、本記述と同等の機能を提供できるプロトコル環境であれば、その種別は問わない。また、記憶サブシステムに関しても、本実施例では、主にディスクアレイを対象に記述したが、記憶装置を可換媒体として置き換え、光ディスクライブラリや、テープライブラリなどに適用することも可能である。更に、ここではホストコンピュータのベンダ単位でグルーピングを行ったが、複数のホストコンピュータ間で共有可能な情報に基づき、任意のグループ分けが可能である。

【0123】以上述べた実施例に基づき、ある記憶サブシステムにおいて本発明が実施されているか否かの確認方法としては、たとえば以下の方法がある。

【0124】①図14あるいは図24に示すような、ホストを一意的に識別する識別子と、論理ユニット番号(LUN)、および仮想的な論理ユニット番号(仮想LUN)を対応づけた管理テーブルを作成する必要がある、またはこの表を参照する処理が行われれば、本発明が実施されている可能性が高い。

【0125】②ファイバモニタを用いて、ホストストレージ間の通信に用いられるコマンドをモニターする。ホストが管理する論理ユニット番号(仮想LUN)と、実際にアクセスした論理ユニットに与えられた、ストレージが管理する論理ユニット番号(LUN)が一致しない場合があれば、本発明が実施されている可能性が高い。

【0126】③ホストが管理する論理ユニット番号(仮想LUN)の絶対値の最大値と、ストレージが管理する論理ユニット番号(LUN)の絶対値の最大値が一致しない場合があれば、本発明が実施されている可能性が高い。(これは、複数のLUに対して、同一の仮想LUNを対応づけることが可能であることによる。)

【0127】

【発明の効果】以上説明したように、管理テーブルを用いることによって、ホストコンピュータにユーザ運用希望にそった形で、記憶サブシステム内の論理ユニットを開示しながら、各ホストコンピュータに対してLU単位にアクセス可否を制限し、不正アクセスを防止するセキュリティ機能を実現できる。更に、記憶サブシステム内のLUに対するアクセス可否判定は、問い合わせコマンド発行時点で判明し、以降この判定を繰り返す必要がないため、記憶サブシステムを高い性能で維持運用しながら、LUに対する強固なセキュリティを確保することができる。

【0128】また、本発明の上記実施例によれば、同一ベンダを示すCompany\_ID等、ホストコンピュータのうちのあるグループに共通な識別情報をWWNから部分的に切り出し、共通の識別情報を持つグループ単位に、記憶サブシステム内のLUにアクセス制限を実施

することで、当該ホストコンピュータ群にのみ有効な記憶資源フォーマットや、アプリケーション、サービス、固有の処理などを提供することができる。

【図面の簡単な説明】

【図1】本発明の実施形態におけるハードウェア構成図である。

【図2】本発明の実施形態におけるフレーム・フォーマットおよびそのフレームヘッダの詳細を示す図である。

【図3】本発明の実施形態におけるフレーム・フォーマットおよびそのフレームヘッダおよびデータフィールドの詳細を示す図である。

【図4】本発明の実施形態におけるログインプロセスを示す図である。

【図5】本発明の実施形態におけるInquiryコマンド送信時のフレーム・フォーマットの詳細を示す図である。

【図6】図5で示したInquiryコマンドに対して送信するInquiryデータ・フォーマットの詳細を示す図である。

【図7】本発明の実施形態におけるInquiryコマンドによる論理ユニットへのアクセス可否問い合わせシーケンスを示す図である。

【図8】本発明の実施形態におけるLUNセキュリティの処理シーケンス概要を示す図である。

【図9】本発明の実施形態における「LUNアクセス管理テーブル」を示す図である。

【図10】本発明を利用しないことによる不完全な「LUNアクセス管理テーブル」のフォーマットおよび、その第一の例を示す図である。

【図11】図10の状態を視覚的に表した図である。

【図12】本発明を利用しないことによる不完全な「LUNアクセス管理テーブル」のフォーマットおよび、その第二の例を示す図である。

【図13】図12で示した状態を視覚的に示した図である。

【図14】本発明の実施形態における「LUNアクセス管理テーブル」のフォーマットおよび、その第一の利用例を示す図である。

【図15】本発明の実施形態における「LUNアクセス管理テーブル」のフォーマットおよび、その第二の利用例を示す図である。

【図16】本発明の実施形態におけるLUNセキュリティの効果を視覚的に示す図である。

【図17】本発明の実施形態における「LUNアクセス管理テーブル」の作成シーケンスを示す図である。

【図18】本発明の実施形態における「WWN-S\_ID変換テーブル」の作成シーケンスを示す図である。

【図19】本発明の実施形態における「WWN-S\_ID変換テーブル」の作成シーケンスを示す図である。

【図20】本発明の実施形態におけるLUNセキュリティ

ィのホストコンピュータ送信の Inquiry コマンドに対する LUN アクセス可否判定シーケンスを示す図である。

【図 21】本発明の実施形態における LUN セキュリティのホストコンピュータ送信の Inquiry コマンドに対する LUN アクセス可否判定シーケンスを示す図である。(つづき)

【図 22】本発明の実施形態における LUN セキュリティの各テーブル間の参照関係を示す図である。

【図 23】本発明の実施形態における WWN のフォーマットの一例を示す図である。

【図 24】本発明の実施形態におけるベンダ別「LUN アクセス管理テーブル」のフォーマットおよび、その第一の利用例を示す図である。

【図 25】本発明の実施形態におけるベンダ別 LUN セキュリティの処理シーケンス概要を示す図である。

【図 26】本発明の実施形態におけるベンダ別 LUN セキュリティの各テーブル間の参照関係を示す図である。

【図 27】本発明の実施形態におけるベンダ別「LUN アクセス管理テーブル」のフォーマットおよび、その第二の利用例を示す図である。

【図 28】本発明の実施形態におけるベンダ別 LUN セキュリティの効果を視覚的に示す図である。

【符号の説明】

201 フレーム・フォーマット  
207 フレーム・ヘッダの詳細  
208 S\_ID  
305 データフィールドの詳細  
307 N\_Port\_Name

308 Node\_Name

506 データフィールドの詳細

601 Inquiry コマンドに対して送信する Inquiry データ・フォーマット

604 クオリファイア (3 ビット) の詳細

605~607 クオリファイア (3 ビット)

608 デバイス・タイプコード (5 ビット) の種別

609 デバイス・タイプ

901 不完全な「LUN アクセス管理テーブル」の第一の例

902~904 記憶サブシステムへアクセス管理されたホストコンピュータ 1~3 の WWN

1001 不完全な「LUN アクセス管理テーブル」の第二の例

1101 記憶サブシステム

1201 不完全な「LUN アクセス管理テーブル」の第三の例

1308 記憶サブシステムのポート配下に定義された LUN 群 LUN0~15

1401 「LUN アクセス管理テーブル」の第一の例

1501 「LUN アクセス管理テーブル」の第二の例

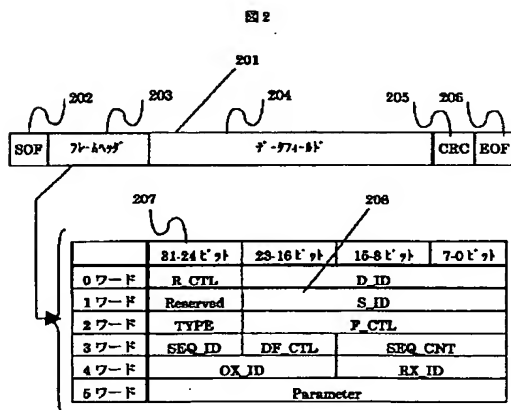
1901 「WWN-S\_ID 変換テーブル」の第一の例

2301 WWN (World Wide Name) のフォーマットの一例

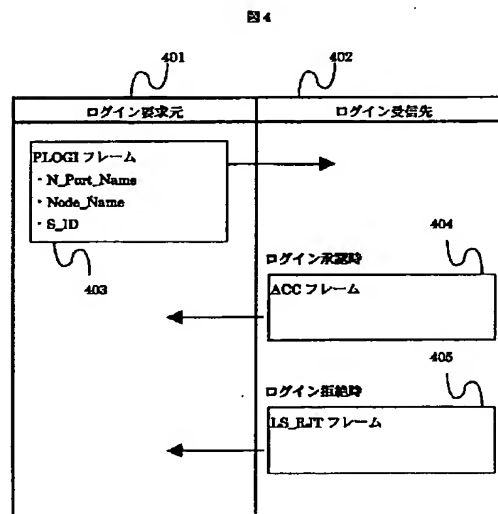
2401 ベンダ別「LUN アクセス管理テーブル」の第一の例

2701 ベンダ別「LUN アクセス管理テーブル」の第二の例

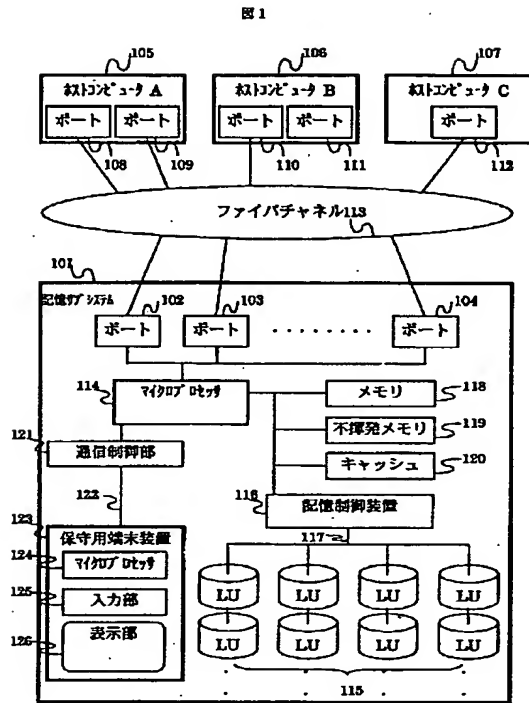
【図 2】



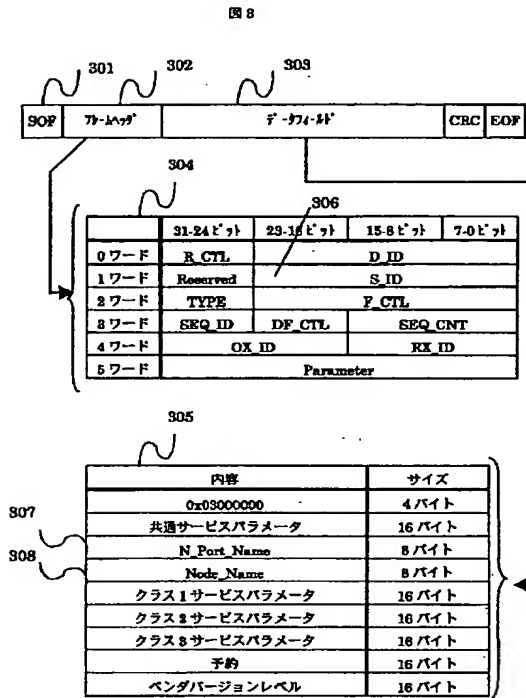
【図 4】



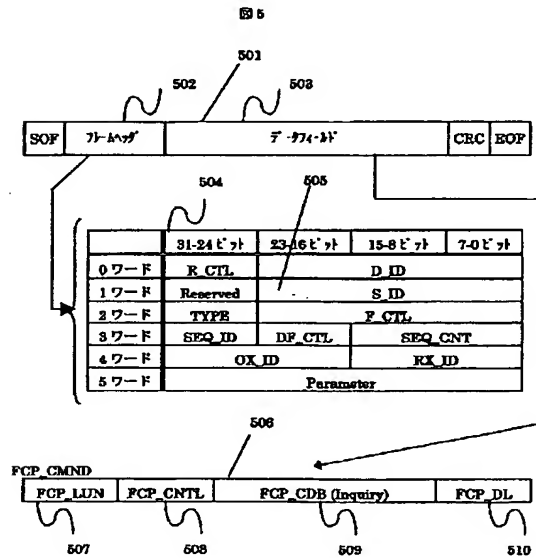
【図1】



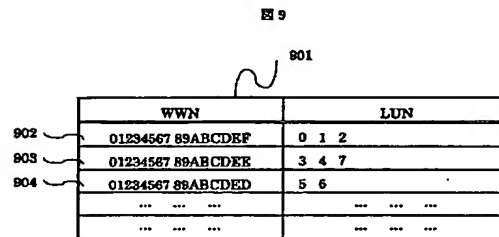
【図3】



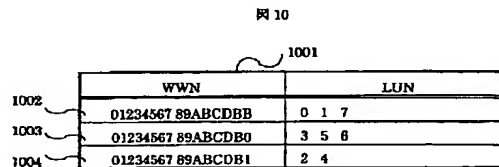
【図5】



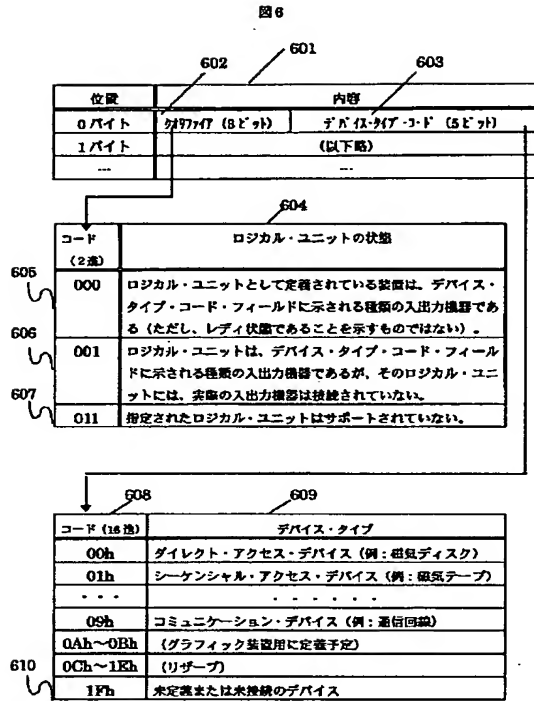
【図9】



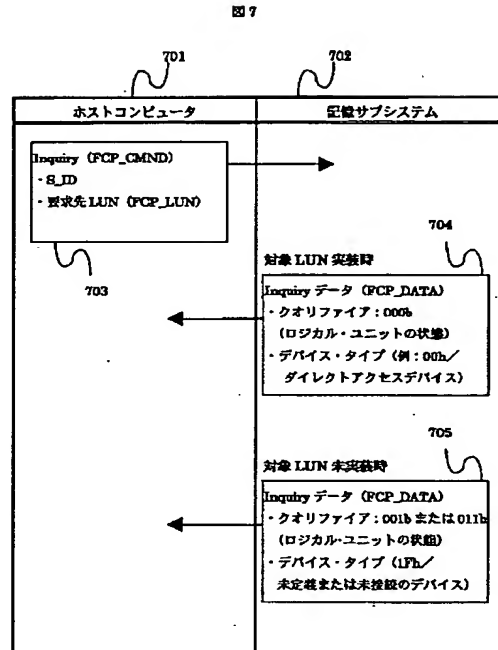
【図10】



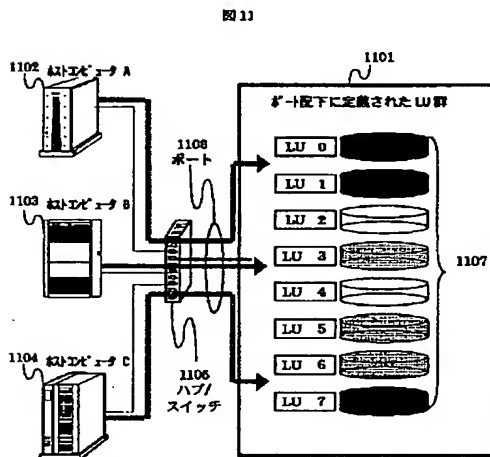
【図6】



【図7】



【図11】



【図12】

図12

WWN	LUN
01234567 89ABCDAA	0 1 2 3 4 5
01234567 89ABCDAB	6 7 8 9 10
01234567 89ABCDAC	11 12 13 14 15

1201 1202 1203 1204

【図15】

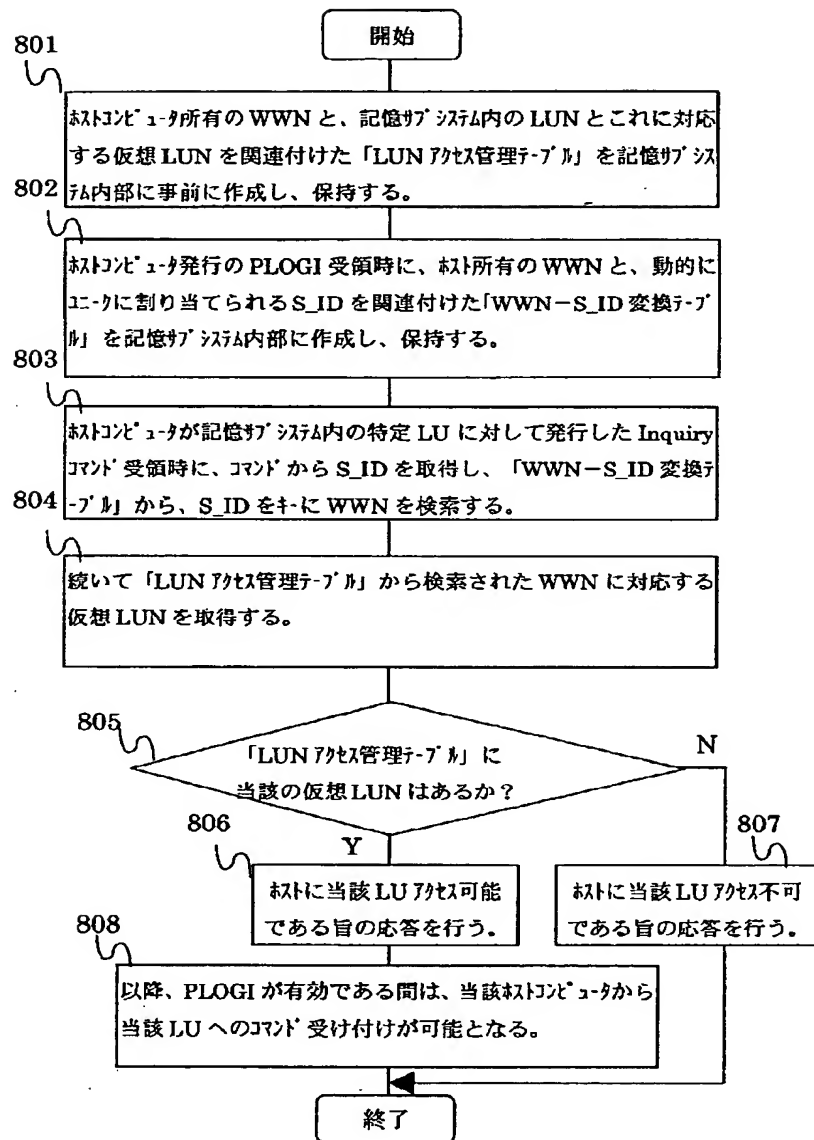
図15

WWN	仮想 LUN	LUN
01234567 89ABCDCC	0 1 2 3 4	0 1 6 8 15
01234567 89ABCDCE	0 1 2	2 7 10
01234567 89ABCDCE	0 1 2 3	3 4 5 14
...	...	...

1501 1502 1503 1504 1505 1506 1507

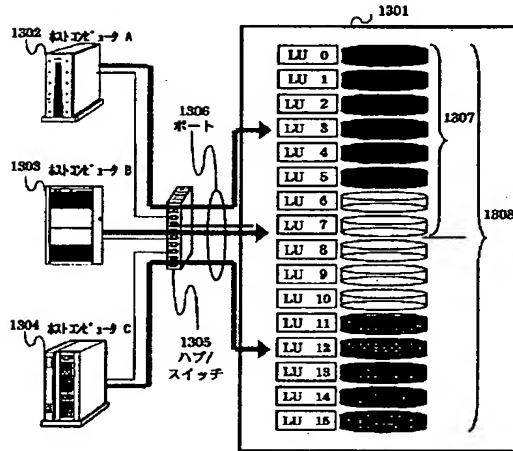
【図8】

図8



【図13】

図 13



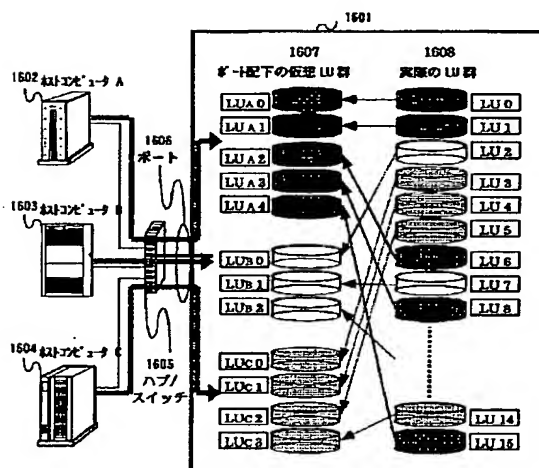
【図14】

図 14

	WWN	仮想 LUN	LUN
1402	01234567 89ABCDEF	0 1 2 3	0 1 2 3
1403	01234567 89ABCDEE	0 1	4 5
1404	01234567 89ABCDEED	0 1	6 7
1405	01234567 89ABCDEEC	0 8 16 24	9 10 11 12
...	...	...	...
1408	01234567 89ABCDCC	16	20
...	...	...	...
1407	01234567 89ABCDHH	0 1 3 5 7	30 31 32 33 34
1408	01234567 89ABCDAA	0 2 4 6	36 38 37 38
...	...	...	...
1409	01234567 89ABCD10	4	39
...	...	...	...
1410	01234567 89ABCD2E	0 1 2 3 4 5	10 11 12 13 14 15
1411	01234567 89ABCD2F	0 1 2 3 4 5	10 11 12 13 14 15
...	...	...	...
1412	01234567 89ABCD31	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15
1413	01234567 89ABCD32	8 9 10 11 12 13 14 15	8 9 10 11 12 13 14 15
...	...	...	...
1414	01234567 89ABCD4E	0 1 2 3	4 8 12 16

【図16】

図 16



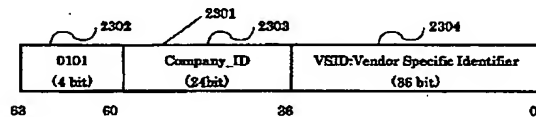
【図19】

図 19

S_ID	WWN
FFFF01	01234567 89ABCDEF
FFFF02	01234567 89ABCDEE
FFFF03	01234567 89ABCDEED
...	...

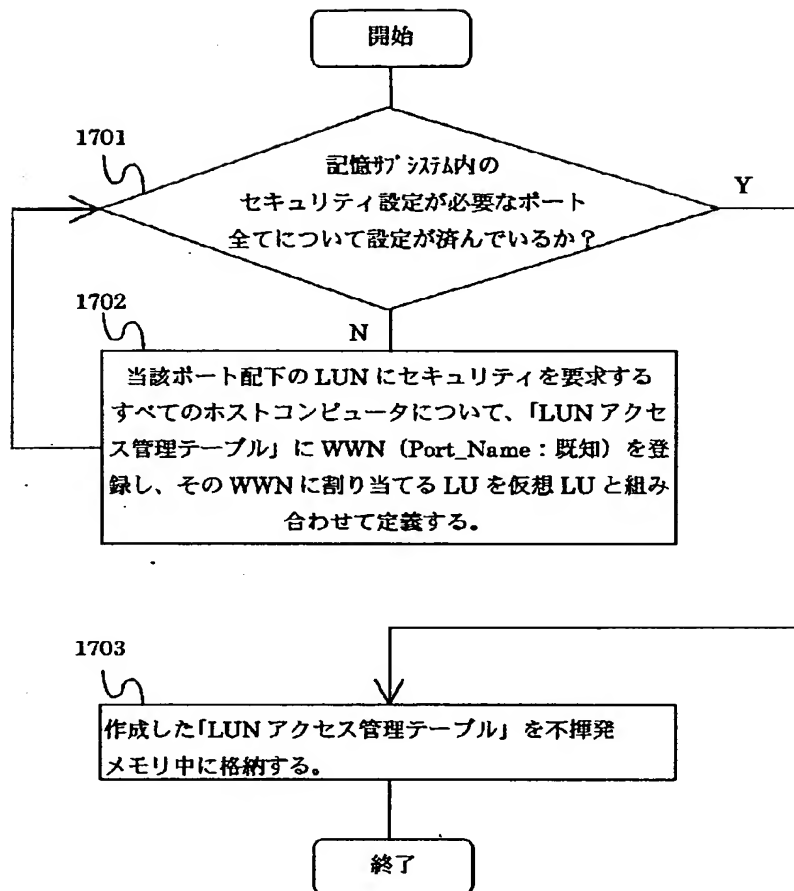
【図23】

図 23



【図17】

図 17



【図24】

図 24

Company ID (hex)	仮想 LUN	LUN
0000E1	0 1 2 3	0 1 2 3
0000E2	0 1	4 5
0000F0	0 1	6 7
000A10	0 8 16 24	9 10 11 12
...	...	...
000011	16	20

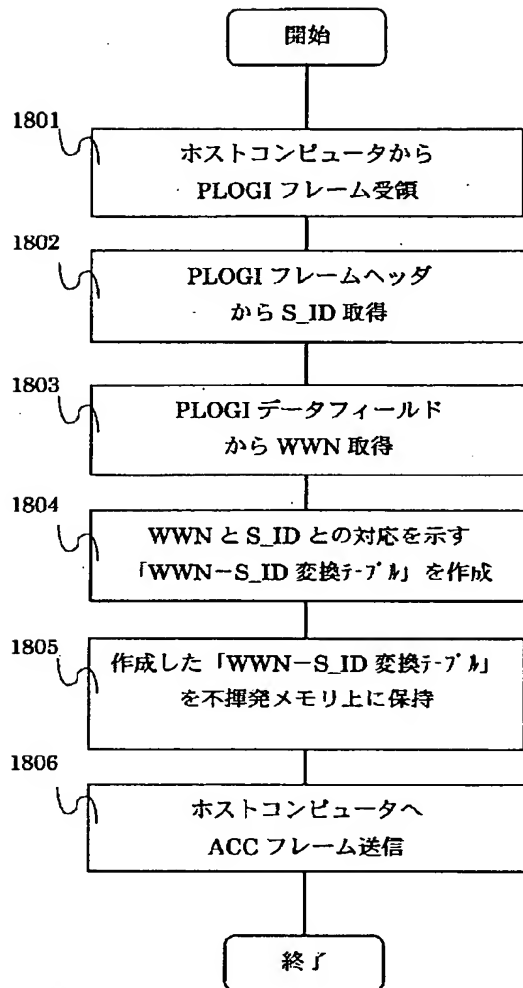
【図27】

図 27

Company ID (hex)	仮想 LUN	LUN
0000E1	0 1 2 3 4	0 1 6 8 15
0000E2	0 1 2	2 7 10
0000F0	0 1 2 3	3 4 5 14
...	...	...

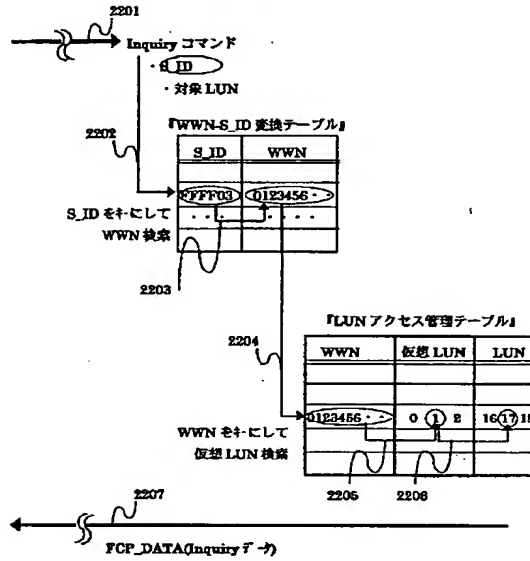
【図18】

図 18



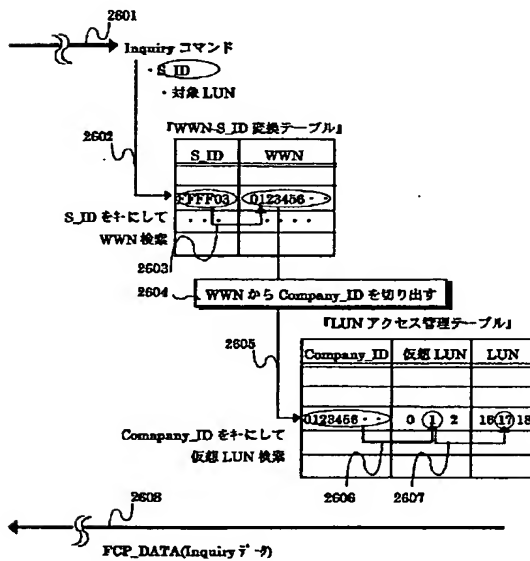
【図22】

図 22



【図26】

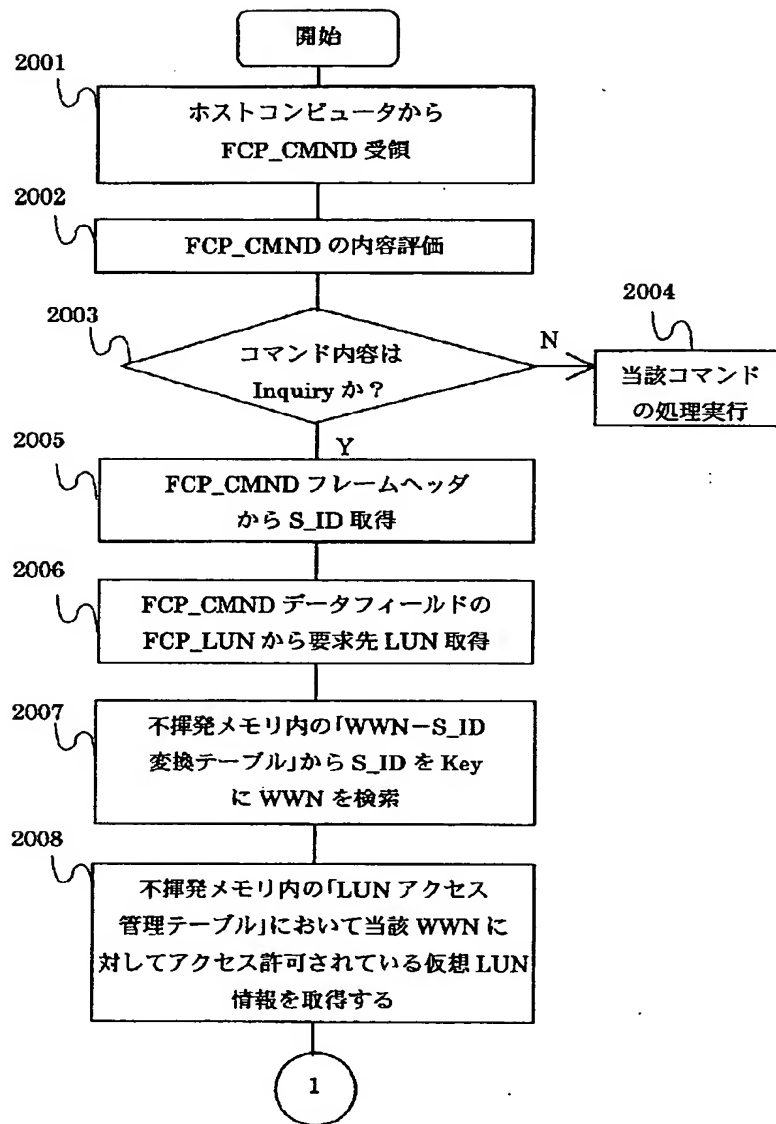
図 26





【図20】

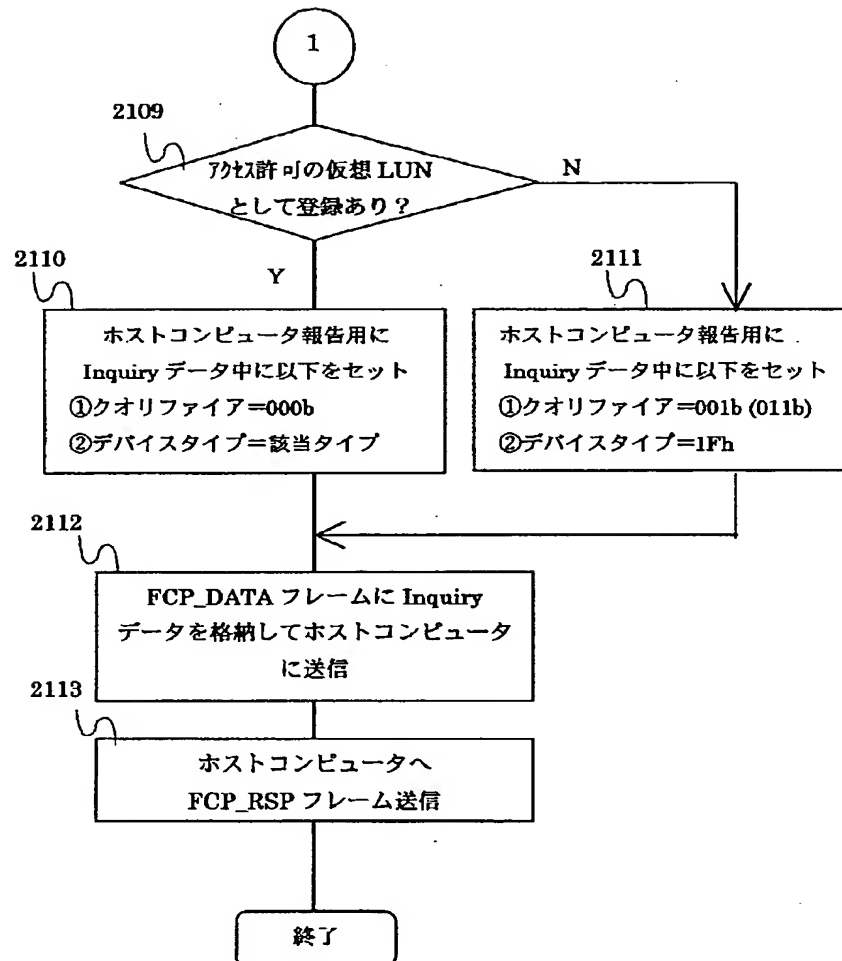
図 20



【図21】

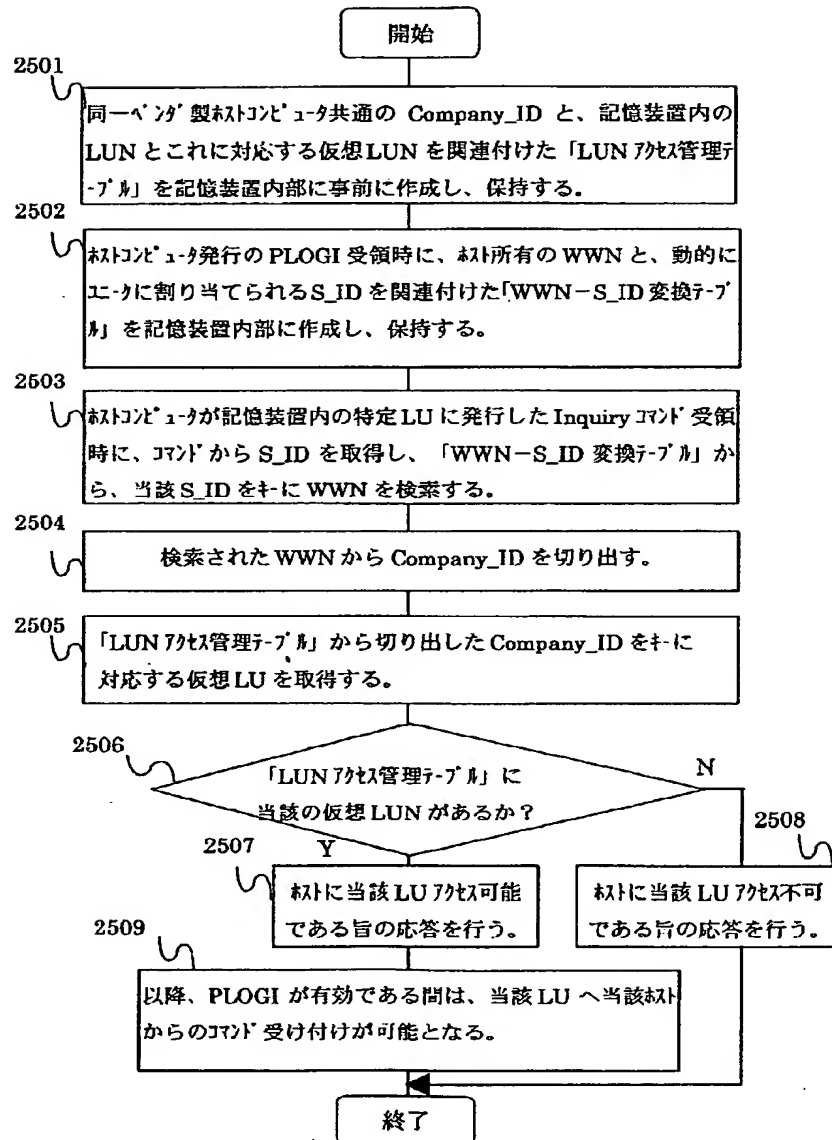
図 21

図 20 のつづき



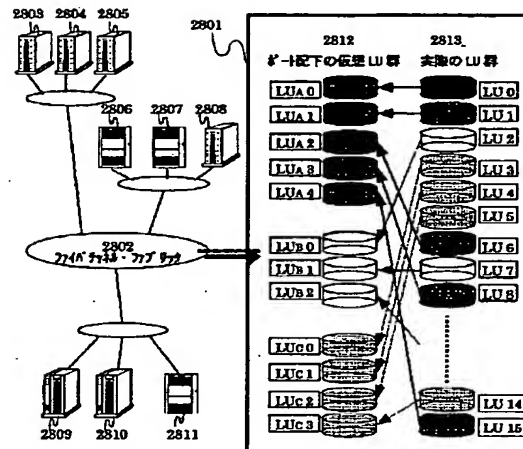
【図25】

図 25



【図28】

図 28



## BEST AVAILABLE COPY

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-333839

(43)Date of publication of application : 18.12.1998

(51)Int.Cl.

G06F 3/06  
 G06F 3/06  
 G06F 12/14  
 H04L 12/56  
 H04L 12/22

(21)Application number : 09-140029

(71)Applicant : HITACHI LTD

(22)Date of filing : 29.05.1997

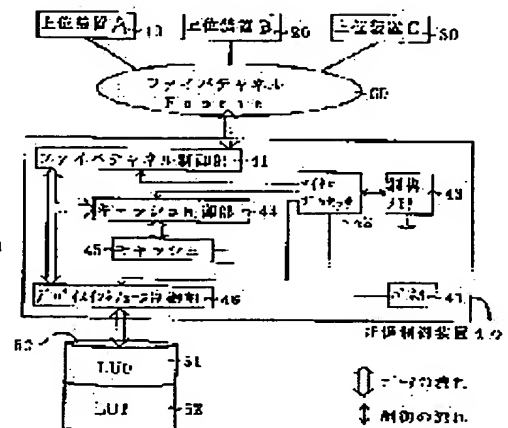
(72)Inventor : SANADA AKIYOSHI  
 NAKANO TOSHIO  
 IWASAKI HIDEHIKO  
 SATO MASAHIKO  
 MURAOKA KENJI  
 TAKAGI KENICHI  
 KOBAYASHI MASAOKI

## (54) FIBER CHANNEL CONNECTION STORAGE CONTROLLER

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a fiber channel connection storage controller having a security function for preventing any illegal access from a host device in an environment in which access from all of host devices can be physically accepted.

**SOLUTION:** N Port Name information for uniquely identifying a host device is set in a microprocessor 42 of a storage controller 40 before the starting of host devices 10, 20, and 30. When the host devices 10, 20, and 30 are started, and an issued frame is received by the storage controller 40, the microprocessor 42 operates comparison to detect whether or not the N Port Name information stored in this frame is registered in an N Port Name list in a control table already set and held in the microprocessor 42, and continues a processing based on the instruction of the frame when they are made coincident, and rejects the request when they are not made coincident. Thus, any illegal access from the host device can be suppressed, and the security can be held.



## LEGAL STATUS

[Date of request for examination]

14.04.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the  
 examiner's decision of rejection or application converted  
 registration]

[Date of final disposal for application]

[Patent number]

3228182

[Date of registration]

07.09.2001

[Number of appeal against examiner's decision of  
 rejection]

[Date of requesting appeal against examiner's decision of  
 rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平10-333839

(43)公開日 平成10年(1998)12月18日

(51)Int.Cl. <sup>6</sup>	識別記号	F I
G 0 6 F 3/06	3 0 4	G 0 6 F 3/06 3 0 4 H
	5 4 0	5 4 0
12/14	3 2 0	12/14 3 2 0 F
H 0 4 L 12/56		H 0 4 L 11/20 1 0 2 A
12/22		11/26
審査請求 未請求 請求項の数 9 O L (全 12 頁)		

(21)出願番号 特願平9-140029

(22)出願日 平成 9 年(1997) 5 月29日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目 6 番地

(72)発明者 眞田 明美

神奈川県小田原市国府津2880番地株式会社

日立製作所ストレージシステム事業部内

(72)発明者 中野 俊夫

神奈川県小田原市国府津2880番地株式会社

日立製作所ストレージシステム事業部内

(72)発明者 岩崎 秀彦

神奈川県小田原市国府津2880番地株式会社

日立製作所ストレージシステム事業部内

(74)代理人 弁理士 高橋 明夫 (外 1 名)

最終頁に続く

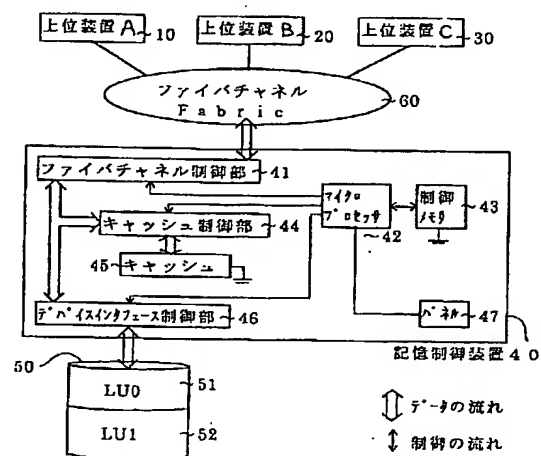
(54)【発明の名称】 ファイバチャネル接続記憶制御装置

(57)【要約】

【課題】 物理的にあらゆる上位装置からのアクセスを受け付けることが可能な環境の中で、上位装置からの不正なアクセスを防止するセキュリティ機能を持つファイバチャネル接続記憶制御装置を提供する。

【解決手段】 上位装置を一意に識別できるN\_Port\_Name情報を、上位装置10、20、30の立ち上がる以前に、記憶制御装置40のマイクロプロセッサ42に設定しておき、上位装置10、20、30が立ち上がり、発行したフレームを記憶制御装置40が受領した際、マイクロプロセッサ42は、当該フレームに格納されているN\_Port\_Name情報が当該マイクロプロセッサ42に既に設定され、保持されている制御テーブル内のN\_Port\_Nameリストに登録されているかどうか、比較を行い、一致した場合は当該フレームの指示に基づく処理を継続し、不一致の場合は要求を拒絶する。これにより、上位装置からの不正アクセスを拒止することができ、セキュリティが保持できる。

図 1



## 【特許請求の範囲】

【請求項1】ANSIX3T11で標準化されたファイバチャネルを、上位装置と記憶制御装置間のインタフェースとし、上位装置、記憶制御装置、及び、記憶制御装置配下の磁気ディスクドライブで構成された記憶装置から成るコンピュータシステムにおいて、

上位装置から発行される、上位装置を一意に識別する情報であるN\_Port\_Name情報を、上位装置の立ち上がる以前に記憶制御装置に設置しておき、記憶制御装置は当該情報を再設定されるまで恒久的に保持する手段を有し、上位装置が立ち上がった後、上位装置が、N\_Port\_Name情報を格納したフレームを記憶制御装置に対して発行し、記憶制御装置がこれを受領した際、既に設定され、保持されている上位装置を一意に識別するN\_Port\_Name情報と、受領したフレームに格納されたN\_Port\_Name情報とを比較する手段を有し、比較により一致した場合、当該フレームの指示に基づく処理を継続し、不一致の場合、受領した当該フレームを拒絶するLS\_RJT(Link Service Reject)フレームを上位装置に返し、上位装置からの不正アクセスを抑止する手段を有することを特徴とするファイバチャネル接続記憶制御装置。

【請求項2】請求項1記載のファイバチャネル接続記憶制御装置において、

当該記憶制御装置が有する上位インタフェース(ポート)の物理的な数以上のN\_Port\_Name情報を設定する手段、すなわち1ポートで複数のN\_Port\_Name情報を設定する手段を有し、ファイバチャネルFabric接続時の論理バス多重構成にも上位装置からの不正アクセスを抑止する手段を有することを特徴とするファイバチャネル接続記憶制御装置。

【請求項3】請求項2記載のファイバチャネル接続記憶制御装置において、

当該記憶制御装置の配下にディスクアレイ装置のように多くの磁気ディスクボリュームを有し、複数のチャネルバスルートを有するシステムにおいて、LUN(ロジカルユニットナンバ)による論理ディスク領域、RAIDグループによる論理ディスク領域、物理ボリューム領域等の記憶領域と、記憶制御装置のポートと、アクセス可能な上位装置のN\_Port\_Name情報とを対応づけて管理する手段を有し、記憶領域毎に不正アクセスを抑止する手段を有することを特徴とするファイバチャネル接続記憶制御装置。

【請求項4】請求項2記載のファイバチャネル接続記憶制御装置において、

当該記憶制御装置配下の記憶装置が、光ディスク装置、光磁気ディスク装置及び磁気テープ装置並びにこれらのライブラリ装置のいずれかである場合に、当該記憶制御装置は、アクセス可能な上位装置、記憶制御装置のポート、記憶装置の対応付けを行い、ライブラリ装置の場合

はさらにドライブ、媒体の対応付けも行って、テーブルで管理、保持する手段を有し、上位装置からの不正アクセスを防止する手段を有することを特徴とするファイバチャネル接続記憶制御装置。

【請求項5】請求項1、2、3、4記載のファイバチャネル接続記憶制御装置において、

上位装置からの不正アクセスを防止するために記憶制御装置が管理する情報は、パネルを用いて設定可能であることを特徴とするファイバチャネル接続記憶制御装置。

【請求項6】請求項1、2、3、4記載のファイバチャネル接続記憶制御装置において、

上位装置からの不正アクセスを防止するために記憶制御装置が管理する情報は、パネルを用いて設定可能であり、さらに、当該情報の設定時の保護策を具備していることを特徴とするファイバチャネル接続記憶制御装置。

【請求項7】請求項1、2、3、4記載のファイバチャネル接続記憶制御装置において、

上位装置からの不正アクセスを防止するために記憶制御装置が管理する情報は、上位装置のユーティリティプログラムを用いて設定可能であることを特徴とするファイバチャネル接続記憶制御装置。

【請求項8】請求項1、2、3、4記載のファイバチャネル接続記憶制御装置において、

上位装置からの不正アクセスを防止するために記憶制御装置が管理する情報は、上位装置のユーティリティプログラムを用いて設定可能であり、さらに、当該情報の設定時の入力保護策を具備していることを特徴とするファイバチャネル接続記憶制御装置。

【請求項9】ネットワークアーキテクチャ形のチャネルを、複数の上位装置と、記憶制御装置との間のインタフェースとし、上位装置、記憶制御装置、及び、記憶制御装置配下の記憶装置から成るコンピュータシステムにおいて、

上位装置を一意に識別できる上位装置識別情報を、複数の上位装置の立ち上がる以前に、記憶制御装置に設定しておき、上位装置が立ち上がり、上位装置識別情報を格納しているフレームを発行し、当該フレームを記憶制御装置が受領した際、記憶制御装置は、当該フレームに格納されている上位装置識別情報が当該記憶制御装置に既に設定されているかどうか、比較を行い、一致した場合は当該フレームの指示に基づく処理を継続し、不一致の場合は要求を拒絶することを特徴とするチャネル接続記憶制御装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ANSIX3T11で標準化されたファイバチャネルを上位装置とのインタフェースとする記憶制御装置に関し、特に上位装置、記憶制御装置及び当該記憶制御装置配下の記憶装置から成るコンピュータシステムにおいて、上位装置から当該



記憶制御装置に当該記憶装置へのアクセス要求があった際の、不正アクセス防止を行う記憶制御装置に関する。

【0002】

【従来の技術】ネットワーク上の不正アクセス防止に関しては、従来から種々の技術が知られている。

【0003】例えば、特開平3-152652号公報には、TCP/IPをサポートするコンピュータシステム間のネットワークセキュリティシステムとして、ログインできるユーザIDをメモリに定義しておくことにより、定義されたユーザID以外でログインしようとすると、そのネットワークを切断する機能を持たせることが開示されている。

【0004】また、特開昭63-253450号公報には、中央処理装置のオペレーティングシステムがユーザID、パスワード、回線アドレスをチェックすることにより、ディスク装置のファイルへの不正アクセス防止を行なうことが示されている。

【0005】さらに、IBM社のESCONインタフェースでは、上位装置が当該上位装置の論理アドレスをソースアドレスとしてフレームに格納し、送信してくることを利用して、記憶制御装置が事前に記憶制御装置に設定した論理アドレスとフレーム内の論理アドレスが一致するか否かをチェックする機能を設けている。

【0006】上述した従来技術は、上位論理層に1種類のレイヤを搭載するインタフェースを対象とした不正アクセス防止手段の域を出ないものである。

【0007】しかし、ANSIX3T11で標準化されたファイバチャネルは、ネットワーク形アーキテクチャであり、上位論理層にはTCP/IP、SCSI、ESCON、IPI等の種々のレイヤを搭載可能である。すなわち、データのフォーマットや内容には無関係に一台の装置から別の装置へバッファの内容を移すため、他のインタフェースと論理的に互換性を持ち、物理的に自由にアクセス可能である。特に、このファイバチャネルと、ディスクアレイ装置等の複数の記憶領域を有する記憶装置とを備えた記憶システムにおいては、上記記憶領域は多くの上位装置に共用される。したがって、従来の不正アクセス防止策では不十分であり、ユーザが意識したセキュリティ設定により、機密保持を行なう必要がある。

【0008】

【発明が解決しようとする課題】本発明は、ANSIX3T11で標準化されたファイバチャネルを、上位装置と記憶制御装置間のインタフェースとし、上位装置、記憶制御装置、及び、この記憶制御装置配下の記憶装置から成るコンピュータシステムにおいて、物理的にあらゆる上位装置からのアクセスを受け付けることが可能な環境の中で、上位装置からの不正なアクセスを拒絶する手段を持たなかった記憶制御装置に対し、上位装置からの不正なアクセスを防止するセキュリティ機能を持つファイバチャネル接続記憶制御装置を提供することを目的とする。

【0009】さらに、本発明は、上位装置からの不正アクセス防止のために、アクセス可能な上位装置を容易に管理できる方式を持つファイバチャネル接続記憶制御装置を提供することを目的とする。

【0010】

【課題を解決するための手段】本発明によれば、上記目的は、アクセス可能な上位装置の、上位装置を一意に識別するN\_Port\_Name情報を当該記憶制御装置に設定し、上位装置から送られてくるフレーム内に格納されたN\_Port\_Name情報と比較し、アクセスの可否を決定することにより達成される。

【0011】上記目的を達成するための本発明の具体的な特徴は、上位装置から発行される、上位装置を一意に識別する情報であるN\_Port\_Name情報を、パネル等を用いて入力し、入力情報を記憶制御装置の制御メモリに、制御テーブルとして格納する手段を有することである。この際、記憶制御装置は当該情報を再設定されるまで恒久的に保持する手段を有することが望ましい。

【0012】そして、上記制御テーブルを不揮発制御メモリに格納するようにすれば、万一の電源瞬断時にも管理情報を守ることができる。

【0013】さらに、本発明の具体的な特徴によれば、上位装置が立ち上がった後、上位装置がN\_Port\_Name情報を格納したフレームを記憶制御装置に対し発行し、記憶制御装置がこれを受領した際、記憶制御装置は既に設置され、保持されている上位装置を一意に識別するN\_Port\_Name情報と、受領したフレームに格納されたN\_Port\_Name情報とを比較する手段を有し、比較により一致した場合は、記憶制御装置は当該フレームの指示に基づく処理を継続し、不一致の場合は、受領した当該フレームを拒絶するLS\_RJTフレームを上位装置に返すようにしたことである。これにより、記憶制御装置は上位装置からの不正アクセスを抑止することができる。

【0014】さらに、本発明の具体的な特徴によれば、当該記憶制御装置が有する上位インタフェース（ポート）の物理的な数以上のN\_Port\_Name情報を設定する手段を有することである。すなわち、1ポートで複数のN\_Port\_Name情報を設定する手段を有することである。これにより、ファイバチャネルファブリック（Fabric）またはスイッチ接続時の論理バス多重構成に対応できる。

【0015】また、当該記憶制御装置の配下に、ディスクアレイ装置のような、多くの磁気ディスクボリュームを有し、複数のチャネルバスルートに有するシステムにおいては、チャネルバスルート毎に、当該記憶制御装置配下のLUN（ロジカルユニットナンバ）による論理ディ

スク領域、物理ボリューム領域、RAIDグループによる論理ディスク領域等の記憶領域と、記憶制御装置のポート、上位装置のN\_Port\_Name情報との対応付けを記憶制御装置内で管理する手段を有することである。これにより、ユーザは、記憶領域毎に、不正アクセスを防止することができ、木目細かいアクセス管理が可能となる。

【0016】さらに、本発明においては、記憶制御装置配下の記憶装置が磁気ディスク装置、ディスクアレイ装置の代わりに、光ディスク装置、光磁気ディスク装置及び磁気テープ装置並びにこれらの各種ライブラリ装置の何れの場合でも、当該記憶制御装置は、アクセス可能な上位装置のN\_Port\_Name情報、記憶制御装置のポート、記憶装置の対応付けを行い、ライブラリ装置の場合はさらにドライブ、媒体の対応付けも行って、制御テーブルで管理、保持する手段を有し、フレーム受領の際にフレーム内の情報と制御テーブル内の情報を比較する手段を有し、上位装置からの不正アクセスの防止を行うことができる。

【0017】さらに、本発明では、記憶制御装置が管理する情報を、パネル等を用いて設定する際、パスワードを入力する等により、管理情報を保護する手段を具備する。これにより、ユーザは当該情報の不正な登録、不正な再設定を防止することができる。また、ユーザは管理情報の設定を行うだけで、容易に不正アクセスを防止可能であり、ユーザの負担が少ない。

【0018】なお、本発明において、記憶制御装置が管理する情報を設定する手段として、上述のように、パネル等を用いて設定する他に、上位装置のユーティリティプログラムを用いて設定することも可能である。

【0019】

【発明の実施の形態】以下、本発明の実施の形態について図面を用いて説明する。まず、図1ないし図5を用いて、本発明の対象となるファイバチャネル及びそれを用いて構成した記憶システムについて説明する。

【0020】図1は、記憶制御装置配下の記憶装置がディスクアレイ装置の場合の記憶システムのハードウェア構成図である。図1において、10、20、30は、データ処理を行う中央処理装置としての上位装置である。

【0021】40は、本発明を実施したディスクアレイ装置の記憶制御装置である。図1に示すように、記憶制御装置40は、上位装置10、20、30との間のデータ転送を制御するためのDMA（ダイレクト アクセス メモリ）を含むプロトコルプロセッサであるファイバチャネル制御部41、記憶制御装置全体を制御するマイクロプロセッサ42、制御装置の動作を制御するマイクロプログラム及び制御用データを保存する制御メモリ43、キャッシュへのデータの読み書きを制御するキャッシュ制御部44、書き込みデータ及びディスクドライブからの読み出しデータを一時バッファリングしておくデ

ィスクキャッシュ45、ディスクドライブとの間のデータ転送を制御するためのDMAを含むプロトコルプロセッサであるデバイスインタフェース制御部46、装置構成情報を記憶制御装置へ入力するパネル47から構成されている。

【0022】50は、記憶制御装置40の配下にあるディスクアレイ装置である。ディスクアレイ装置50は、上位装置のデータを格納する装置で、複数台の個別ディスクを冗長性を持つように配置構成したものである。

【0023】ディスクアレイ装置50を構成するディスクは、論理的に分割し、分割した区画をそれぞれ異なるRAIDレベルに設定することができる。この区画をRAIDグループという。このRAIDグループをさらに論理的に分割したSCSIのアクセス単位である領域をLU（Logical Unit）といい、その領域は、各々、LUN（Logical Unit Number）という番号を持つ。本実施の形態ではディスクアレイ装置50は、LUN0番のLUである、LU0（51）とLUN1番のLUである、LU1（52）の2個の領域を有する場合を示している。

【0024】なお、LUの数は、図1に示す2個に限らずもっと多くてもよく、シングルターゲット機能の場合、ターゲット当たり最大8個までLUを設定できる。

【0025】また、本実施の形態では、LUなる記憶領域をアクセス単位としているが、アクセス単位とする記憶領域としては、物理ボリューム単位やRAIDグループ単位の記憶領域も可能である。

【0026】上位装置10、20、30と記憶制御装置40は、ファイバチャネル60をインタフェースとし、ファブリック（Fabric）という装置を介して接続されている。

【0027】図1のシステムの動作を、上位装置10が記憶制御装置40経由でディスクアレイ装置50とデータ転送を行う場合を例にとり、制御の流れ、データの流れを中心に説明する。

【0028】上位装置10がアクセス要求を出すと、その要求を認識したファイバチャネル制御部41はマイクロプロセッサ42に割り込み要求を発行する。マイクロプロセッサ42は、上位装置からのコマンド情報及び本発明で必要な制御情報を、制御メモリ43に格納する。

【0029】コマンド情報が、ライトコマンドの場合は、マイクロプロセッサ42はファイバチャネル制御部41にデータ転送を指示し、転送されたデータをキャッシュ制御部44を経由してキャッシュ45に格納する。上位装置10に対しては、ファイバチャネル制御部41がライト完了報告を行う。ライト完了報告後、マイクロプロセッサ42がデバイスインタフェース制御部46を制御し、ディスクアレイ装置50に対し、データ及び冗長データを書き込む。この場合、一般のRAID5の動作においては、旧データ、旧パリティ及び新データに基

いて新バリティを作成するが、本発明の制御によれば、マイクロプロセッサ42が、デバイスインタフェース制御部46及びキャッシュ制御部44、制御メモリ43、キャッシュ45を用いて行なう。

【0030】一方、上位装置10からコマンド情報として、リードコマンド情報を受けた場合は、マイクロプロセッサ42は、デバイスインタフェース制御部46に指示を出し、当該アクセス要求のデータブロックが格納されたディスクアレイ装置50へアクセスしてデータを読み出し、キャッシュ制御部44を経由してキャッシュ45へデータを格納する。マイクロプロセッサ42は、ファイバチャネル制御部41に指示を出し、ファイバチャネル制御部41は、キャッシュ45に格納したデータを上位装置10に転送し、転送後上位装置へリード完了報告を行なう。

【0031】次にファイバチャネル60の特長を説明する。ファイバチャネルは最大10kmの距離で100MB/sの転送が可能な高速インタフェースである。ファイバチャネルのアーキテクチャは転送元のバッファから転送先のバッファへデータを送るが、データのフォーマットや内容には無関係に一台の装置から別の装置へバッファの内容を移すため、異なるネットワーク通信プロトコルを処理するオーバーヘッドがなく、高速データ転送を実現している。上位論理層にはTCP/IP、SCSI、ESCON、IPI等の種々のレイヤを搭載可能である。すなわち、他のインタフェースと論理的に互換性を持つ。複雑な装置間の接続/交換という機能はFabricと呼ぶ装置が行ない、論理バス多重構成を組むことが可能である。

【0032】ファイバチャネルがデータをやりとりする基本単位をフレームと言う。次に、このフレームについて、図2を用いて説明する。

【0033】図2に示すように、フレーム70は、スタートオブフレームSOF(Start Of Frame)71、フレームヘッダ72、データフィールド73、サイクリックリダンダンシチェックCRC(Cyclic Redundancy Check)74及びエンドオブフレームEOF(End Of Frame)75で構成される。

【0034】SOF71は、フレームの先頭に置く4バイトの識別子である。

【0035】EOF75は、フレームの最後につける4バイトの識別子で、SOF71とEOF75によりフレームの境界を示す。ファイバチャネルではフレームがない時はアイドル(idle)という信号が流れている。

【0036】フレームヘッダ72は、フレームタイプ、上位プロトコルタイプ、送信元と送信先のN\_Port\_ID情報、N\_Port\_Name情報等を含む。N\_Port\_IDはアドレスを表わし、N\_Port\_Nameはポートの識別子を表わす情報である。

【0037】データフィールド73の先頭部には上位レイヤのヘッダを置くことができる。これにデータそのものを運ぶペイロード部が続く。CRC74は、フレームヘッダとデータフィールドのデータをチェックするための、4バイトのチェックコードである。

【0038】上記フレームヘッダ72のフォーマット80を、図3に示す。フレームヘッダフォーマット80において、デスティネーションアイデンティファイアD\_ID(Destination ID)81はフレーム受け取り側のアドレス識別子であり、また、ソースアイデンティファイアS\_ID(Source ID)82はフレーム送信側のN\_Portアドレス識別子であり、各々、N\_Port\_ID、N\_Port\_Name情報等を含む。

【0039】次に図4を用いて、フレームを構成するデータフィールド73のペイロードの1つである、ファイバチャネルプロトコルコマンドFCP\_CMND(Fibre Channel Protocol for SCSI Command)のペイロード90の説明を行なう。

【0040】FCPロジカルユニットナンバFCP\_LUN(FCP Logical Unit Number)フィールド91には、コマンドを発行するロジカルユニット番号LUNが指定される。FCPコントロールFCP\_CNTL(FCP Control)フィールド92には、コマンド制御パラメータが指定される。そして、FCPコマンドデスク립タブロックFCP\_CDB(FCP Command Descriptor Block)フィールド93には、SCSIコマンドデスク립タブロック(SCSI Command Descriptor Block)が格納され、リードコマンドRead等のコマンド種類、LUN等のアドレス、ブロック数が示される。FCPデータレングスFCP\_DL(FCP Data Length)フィールド94には、当該コマンドにより転送されるデータ量がバイト数で指定される。

【0041】以上のように構成されたフレームによってデータのやりとりが行われる。

【0042】フレームは機能に基づいてデータフレームとリンク制御フレームとに大別される。データフレームは、情報を転送するために用い、データフィールドのペイロード部に上位プロトコルで使用するデータ、コマンドを搭載する。

【0043】一方、リンク制御フレームは、一般に、フレーム配信の成功あるいは不成功を示すのに使われる。フレームを1個受領したことを示したり、ログインする場合に転送に関するパラメータを通知したりするフレーム等がある。

【0044】次に、図5を用いて、「シーケンス」について説明する。ファイバチャネルにおけるシーケンス

は、あるN\_Portから別のN\_Portへ、一方方向に転送される関連するデータフレームの集まりのことを言い、SCSIのフェーズに相当する。シーケンスの集まりをエクスチェンジと呼ぶ。例えばコマンドを発行して、そのコマンドの終了までに、そのコマンド実行のためにやりとりされるシーケンスの集まり（コマンド発行、データ転送、終了報告）がエクスチェンジとなる。このように、エクスチェンジはSCSIのI/Oに相当する。

【0045】図5(a)、(b)及び(c)は、それぞれ、ログインシーケンス(100)、リードコマンドシーケンス(110)及びライトコマンドシーケンス(120)を示す。

【0046】ファイバチャネルインタフェースでは、上位装置がデバイスに対し、通信パラメータを含むポートログインPLOGI(N\_Port Login)フレームを送り、デバイスがこれを受け付けることで通信が可能となる。これをログインと呼ぶ。図5(a)に、ログインシーケンス(100)を示す。

【0047】図5(a)のログインシーケンス(100)において、まず、シーケンス101で、上位装置はデバイスに対し、PLOGIフレームを送り、ログインの要求を行なう。デバイスはアクノレッジACK(Acknowledge)フレームを上位装置に送り、PLOGIフレームを受け取ったことを知らせる。

【0048】次いで、シーケンス102において、デバイスは、ログイン要求を受け付ける場合はアクセプトACC(Accept)フレームを、要求を拒絶する場合はリンクサービスリジェクトLS-RJT(Link Service Reject)フレームを、それぞれ、上位装置に送る。

【0049】次に、図5(b)のリードコマンドのシーケンス(110)を説明する。

【0050】シーケンス111において、上位装置はデバイスに対し、FCP\_CMNDフレームを送り、リード要求を行なう。デバイスはACKフレームを上位装置に送る。

【0051】シーケンス102では、デバイスは、FCPトランスファレディFCP\_XFER\_RDY(FCP Transfer Ready)フレームを上位装置に送り、データ転送の準備ができたことを知らせる。上位装置はACKフレームをデバイスに送る。

【0052】シーケンス113に進み、デバイスはFCPデータ(FCP\_DATA)フレームを上位装置に送り、データを転送する。上位装置はACKフレームをデバイスに送る。

【0053】次のシーケンス114では、デバイスはFCP\_RSPフレームを上位装置に送り、データの転送が正常終了したことを知らせる。上位装置はACKフレームをデバイスに送る。

【0054】次に、図5(c)のライトコマンドのシーケンス(120)を説明する。

【0055】シーケンス121において、上位装置はデバイスに対し、FCP\_CMNDフレームを送り、ライト要求を行なう。デバイスはACKフレームを上位装置に送る。

【0056】次いで、シーケンス122において、デバイスはFCP\_XFER\_RDYフレームを上位装置に送り、データ書き込みが可能であることを知らせる。上位装置はACKフレームをデバイスに送る。

【0057】さらに、シーケンス123において、上位装置はFCP\_DATAフレームをデバイスに送り、データを転送する。デバイスはACKフレームを上位装置に送る。

【0058】最後に、シーケンス123において、デバイスは、FCPレスポンスFCP\_RSP(FCP Response)フレームを上位装置に送り、データの受け取りが正常終了したことを知らせる。上位装置はACKフレームをデバイスに送る。

【0059】以上、図1ないし図5によって、一般的なシステム構成、フォーマット及びシーケンスを説明したが、以下、本発明によるセキュリティチェックについて説明する。

【0060】初めに、PLOGI時におけるN\_Port\_Name情報をを用いたセキュリティチェックについて、説明を行なう。

【0061】本発明では、図1において、まず、上位装置10、20、30の立ち上がる以前に、ユーザは記憶制御装置40のマイクロプロセッサ42にアクセス可能な上位装置のリストを設定する。すなわち、上位装置を識別できるN\_Port\_Name、N\_Port\_ID等の情報を、パネル47を用いて入力する。この際、パネルへの入力上の機密保護機能を実現するために、入力に際してパスワードを要求し、セキュリティを強化できる。

【0062】パスワードを入力し、既に設定したパスワードとの一致が図られた場合、記憶制御装置のポート毎にアクセス可能な上位装置のN\_Port\_Name情報を入力し、入力情報を制御テーブルに格納する。

【0063】いま、例として、上位装置10、20はディスクアレイ装置50にアクセス可能、上位装置30はディスクアレイ装置50にはアクセス不可能とし、N\_Port\_Nameを、上位装置10はHOSTA、上位装置20はHOSTB、上位装置30はHOSTCとし、記憶制御装置40のファイバチャネル制御部41のポートをCTLOP0とした場合、ログイン要求制御テーブル130は、図6のようになる。

【0064】図6に示すこのログイン要求制御テーブル130を、不揮発メモリ上に設定することにより、万一の電源瞬断時にも管理情報を守ることができる。

【0065】また、ログイン要求制御テーブル130に格納した情報は、電源を切断した場合はハードディスク領域50へ格納する。または情報の更新時にメモリ43とディスク50へ反映を行なう。これにより記憶制御装置40は、当該情報を再設定されるまで恒久的に保持することができる。

【0066】なお、ファイバチャネルにおいてノードやポートの識別に使用される自ノード情報として、N\_Port\_Nameの他に、N\_Port\_IDがあるが、N\_Port\_IDは変更される可能性があり、ユーザが管理する数値ではないため、N\_Port\_Name情報をセキュリティのためのチェック対象とするのが望ましい。

【0067】次に、図1及び図7を用いて上位装置のログイン要求に対する記憶制御装置のフレーム処理手順の説明を行なう。

【0068】(ステップS71) 上位装置10、20、30が立ち上がり、各々、N\_Port\_Name情報を格納したログイン要求フレームであるPLOGIフレームを発行する。記憶制御装置40のマイクロプロセッサ42は、当該フレームを受領すると、まずこのフレームを受領したことを示すACKフレームを各上位装置に返す。

【0069】(ステップS72) そしてマイクロプロセッサ42は、当該フレームに格納されているN\_Port\_Name情報を切り出し、そのN\_Port\_Name情報が、既に設定され、保持されている制御テーブル内のN\_Port\_Nameリストに登録されているかどうか、比較を行なう。

【0070】(ステップS73) (ステップS74) (ステップS75)

上位装置10、20の発行した当該フレームに格納されているN\_Port\_Name情報は、制御テーブル内に登録されているN\_Port\_Name情報と一致するため、記憶制御装置40のマイクロプロセッサ42は、上位装置10、20に対してはログイン要求を受け付けた印として、ACCフレームを返し、ログイン処理を続行する。

【0071】(ステップS73) (ステップS76) 一方、上位装置30の発行した当該フレームに格納されているN\_Port\_Name情報は、制御テーブル内に登録されているN\_Port\_Name情報と一致しないため、記憶制御装置40のマイクロプロセッサ42は、上位装置30に対しては接続を拒絶するリジェクトパラメータをいれたLS\_RJTフレームを返す。

【0072】以上のように、記憶制御装置40が、ログイン要求制御テーブル130を用いて、上位装置と記憶制御装置のポートの対応付けを管理することにより、ユーザはポート毎に上位装置からの不正アクセスを抑止ことができ、セキュリティが保持できる。

【0073】次に、本発明において、ディスクアレイ装置の記憶領域であるLUN毎に、N\_Port\_Name情報を用いてセキュリティチェックを実施する方法について説明する。

【0074】本発明では、まず上位装置10、20、30の立ち上がる以前に、記憶制御装置40のマイクロプロセッサ42に、LUN毎にアクセス可能な上位装置のリストを設定する。上位装置を識別できるN\_Port\_Name、N\_Port\_ID等の情報を、パネル47を用いて入力する。この際、パネル47への入力上の機密保護機能を実現するために、入力に際してパスワードを要求し、セキュリティを強化することができる。

【0075】パスワードを入力し、既に設定したパスワードとの一致が図られた場合、LUN毎に記憶制御装置のポート及びアクセス可能な上位装置のN\_Port\_Name情報を入力し、入力情報を制御テーブルに格納する。

【0076】LU0(51)は、上位装置10から記憶制御装置40のファイバチャネル制御部41のポート経由でアクセス可能、LU1(52)は、上位装置20から記憶制御装置40のファイバチャネル制御部41のポート経由でアクセス可能とし、N\_Port\_Nameを、上位装置10はHOSTA、上位装置20はHOSTB、記憶制御装置40のファイバチャネル制御部41のポートをCTLOP0、とした場合、I/O要求制御テーブル140は、図8のようになる。

【0077】図8に示すこのI/O要求制御テーブル140は不揮発メモリ上に設定すると、万一の電源瞬断時にも管理情報を守ることができる。

【0078】また、図8のI/O要求制御テーブル140に格納した情報は、電源を切断した場合は、ハードディスク領域50へ格納する。または情報の更新時にメモリ43とディスク50へ反映を行なう。これにより記憶制御装置40は当該情報を再設定されるまで恒久的に保持することができる。

【0079】本実施例ではチャネルバスルートは1通りであるが、複数のチャネルバスルートを有するシステムにおいても同様である。

【0080】以下に図1及び図9を用いて、上位装置のI/O要求に対する記憶制御装置のフレーム処理手順の説明を行なう。上記の例ではPLOI時にセキュリティチェックを行なったが、本実施の形態では、各SCSIコマンド毎にチェックを行なう。

【0081】(ステップS91) 上位装置10がLU0(51)にI/O要求を出したい場合、上位装置10は記憶制御装置40に対し、SCSI CDBを格納したフレームを発行する。記憶制御装置40がこのフレームを受領した場合、まず、このフレームを受領したことを示すACKフレームを上位装置10に返す。

【0082】(ステップS92) そしてマイクロプロセ

ッサ42は、当該フレームに格納されているN\_Port\_Name情報及びCDB内のLUN番号を切り出し、そのN\_Port\_Name情報及びLUN番号が、当該マイクロプロセッサ42に既に設定され保持されている制御テーブル内のリストに登録されているかどうか、比較を行なう。

【0083】(ステップS93)(ステップS94)(ステップS95)

管理テーブル内には、「上位装置10は、LU0(51)をアクセス可能である」と登録されているため、記憶制御装置40のマイクロプロセッサ42はコマンドを受領し、I/O処理を継続する。

【0084】(ステップS91)一方、上位装置20が記憶制御装置40にLU0(51)のI/O要求フレームを発行し、記憶制御装置40がこのSCSI CDBを格納したフレームを受領した場合、マイクロプロセッサ42は、まずこのフレームを受領したことを示すACKフレームを上位装置20に返す。

【0085】(ステップS92)そしてマイクロプロセッサ42は、当該フレームに格納されているN\_Port\_Name情報及びCDB内のLUN番号を切り出し、そのN\_Port\_Name情報及びLUN番号が、管理テーブル内にあるかどうかの検索を行なう。

【0086】(ステップS93)(ステップS96)検索を行なった結果、管理テーブル内に、該当するLUNおよびN\_Port\_Nameの組合わせが存在しないため、記憶制御装置40のマイクロプロセッサ42は、上位装置20にLS\_RJTフレームを送って、I/O要求を拒絶する。

【0087】こうして記憶制御装置は不正なアクセスを防止することができる。

【0088】ここではログイン及びI/O要求フレームを取り上げたが、これら以外の他の上位装置フレームに格納されているN\_Port\_Name情報を比較してもよい。

【0089】なお、ファイバチャネル接続記憶制御装置配下の記憶装置がディスクアレイ装置に限らず、光ディスク装置、光磁気ディスク装置及び磁気テープ装置並びにこれらのライブラリ装置である場合にも本発明を適用できる。

【0090】記憶制御装置配下の記憶装置が光ディスクライブラリ装置の場合に本発明を適用した場合の概要を図10を用いて説明する。150は記憶制御装置40配下の光ディスクライブラリ装置であり、151は光ディスクドライブ、152から156は光ディスクの媒体である。

【0091】ユーザは上位装置10、20、30が立ち上る前にパネルを使用して、媒体、ドライブ、ポートとN\_Port\_Name情報との対応付けを設定し、上位装置のアクセス権限をマイクロプログラムに保持して

おく。

【0092】媒体152、153、154は、上位装置10からアクセス可能、媒体155、156は上位装置20からアクセス可能とし、N\_Port\_Nameを上位装置10はHOSTA、上位装置20はHOSTB、記憶制御装置40のポートをCTLOP0、光ディスクドライブ151をDRIVE0、媒体152、153、154、155、156を各々MEDA、MEDB、MEDC、MEDD、MEDE、とした場合、要求制御テーブル160は、図11のようになる。

【0093】各上位装置がI/O要求フレームを発行した際、フレームを構成するペイロード内のCDBにボリューム情報が格納されているため、記憶制御装置40は当該フレームを受領した際、フレーム内のN\_Port\_Name情報及びペイロード内の媒体識別子を、当該記憶制御装置40に既に設定され、保持されている制御テーブルと比較を行なえばよい。このように、本発明を応用することによって、記憶制御装置は上位装置からの不正アクセスを防止可能である。

【0094】

【発明の効果】以上述べたように、本発明によって、ANSIX3T11で標準化されたファイバチャネルを上位装置と記憶制御装置間のインタフェースとし、上位装置、記憶制御装置、及び記憶制御装置配下の記憶装置から成るコンピュータシステムにおいて、不正な上位装置からのアクセスを抑止することができるので、記憶装置内のデータの機密保護を行うことができる。

【0095】また、上位装置、記憶制御装置のポート、記憶領域を対応付けて上位装置からのアクセスを木目細かに管理できるので、記憶領域毎に用途を変える等、記憶装置をニーズに合わせて活用することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態を示すハードウェア構成図である。

【図2】第1の実施の形態におけるフレームのフォーマット図である。

【図3】図2で示したフレームを構成するフレームヘッダのフォーマット図である。

【図4】図2で示したフレームの一つであるFCP\_CMNDのペイロードのフォーマット図(a)及び当該ペイロードを構成するFCP\_CDBのフォーマット図(b)である。

【図5】第1の実施の形態において上位装置とデバイスがデータフレームのやりとりを行なうシーケンスの例を示し、ログイン時のシーケンス図(a)、リードコマンド時のシーケンス図(b)及びライトコマンド時のシーケンス図(c)である。

【図6】第1の実施の形態において、記憶制御装置が、上位装置を管理する制御テーブルを示した図である。

【図7】第1の実施の形態において、記憶制御装置が、上位装置（ホスト）からのログイン要求時に実行するフレーム処理のフローチャートである。

【図8】第1の実施の形態において、記憶制御装置が、記憶領域を管理する制御テーブルを示した図である。

【図9】第1の実施の形態において、記憶制御装置が、ホストからのI/O要求時に実行するフレーム処理のフローチャートである。

【図10】本発明の第2の実施の形態として、記憶制御装置配下の記憶装置が、光ディスクライブラリの場合を示すハードウェア構成図である。

【図11】図10に示す第2の実施の形態において、記憶制御装置が管理する制御テーブルを示した図である。

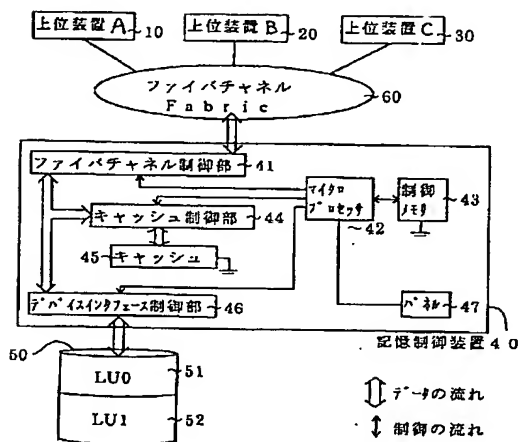
【符号の説明】

10、20、30…上位装置、40…記憶制御装置、41…ファイバチャネル制御部、42…マイクロプロセッサ、43…制御メモリ、44…キャッシュ制御部、45…キャッシュ、46…デバイスインタフェース制御部、47…パネル、50…ディスクアレイ装置、51…ロジカルユニット0、52…ロジカルユニット1、60…ファイバチャネル、70…フレーム、71…スタートオブフレームSOF (Start Of Frame)、72…フレームヘッダ、73…データフィールド、74…サイクリックリダンダンシチェックCRC (Cycli

cRedundancy Check)、75…エンドオブフレームEOF (End Of Frame)、80…フレームヘッダのフォーマット、81…デスティネーションアイデンティファイアD\_ID (Destination ID)、82…ソースアイデンティファイアS\_ID (Source ID)、90…ファイバチャネルプロトコルコマンドFCP\_CMNDペイロード (Fibre Channel Protocol for SCSI Command)、91…ファイバチャネルプロトコルロジカルユニットナンバFCP\_LUN (FCP Logical Unit Number)、92…ファイバチャネルプロトコルコントロールFCP\_CNTL (FCP Control)、93…ファイバチャネルプロトコルコマンドデスク립タブロックFCP\_CDB (FCP Command Descriptor Block)、94…ファイバチャネルプロトコルデータレングスFCP\_DL (FCP Data Length)、100…ログイン、110…リードコマンド、120…ライトコマンド、130…ログイン要求制御テーブル、140…磁気ディスクアレイI/O要求制御テーブル、150…光ディスクライブラリ、160…光ディスクライブラリI/O要求制御テーブル

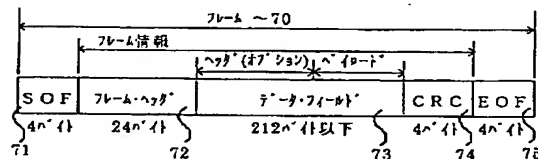
【図1】

図 1



【図2】

図 2



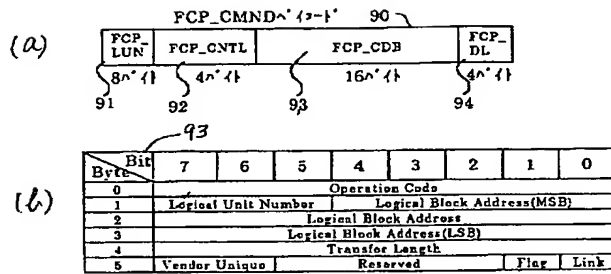
【図3】

図 3

Bit	31-24	23-16	15-8	7-0
0	R_CTL	D_ID (フレーム受け取り側の N_Portアドレス識別子)		
1	Reserved	S_ID (フレーム送信側の N_Portアドレス識別子)		
2	TYPE		F_CTL	
3	SEQ_ID	DF_CTL		SEQ_CNT
4		OX_ID		RX_ID
5	Parameter			

【図4】

図 4



【図6】

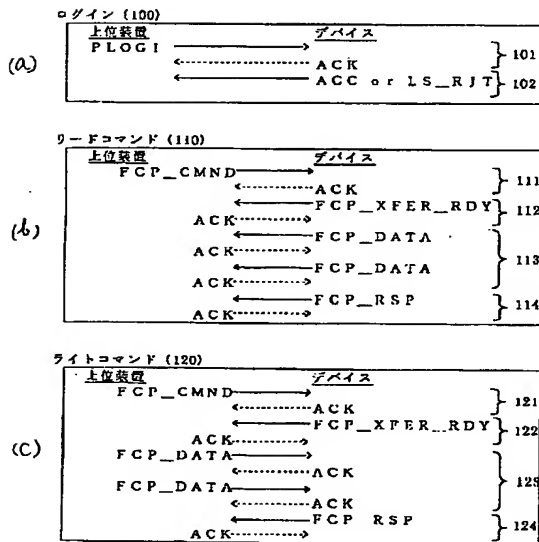
図 6

制御テーブル 130

上位装置の N_Port_Name	記憶制御装置の 上位インタフェース(ポート)
HOSTA	CTL0P0
HOSTB	CTL0P0

【図5】

図 5



【図8】

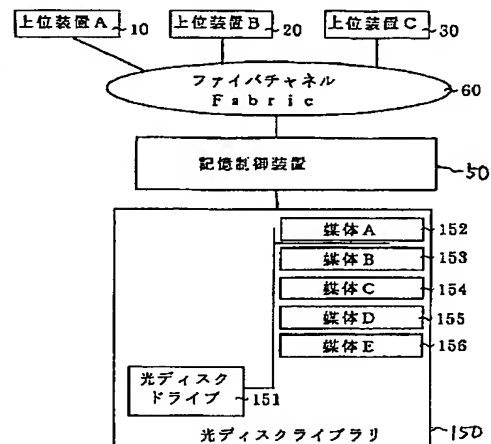
図 8

制御テーブル 140

記憶領域	上位装置の N_Port_Name	記憶制御装置の 上位インタフェース(ポート)
LU0	HOSTA	CTL0P0
LU1	HOSTB	CTL0P0

【図10】

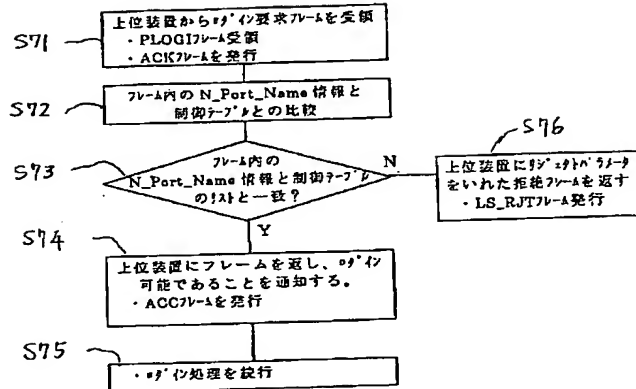
図 10





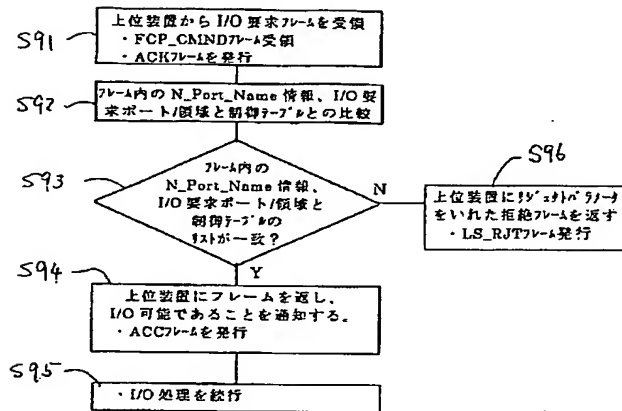
【図7】

図 7



【図9】

図 9



【図11】

図 11

制御テーブル 160

記憶領域 光ディスク媒体	光ディスク ドライブ	上位装置の N_Port_Name	記憶制御装置の 上位インターフェイス(ポート)
MEDA	DRIVE0	HOSTA	CTL0P0
MEDB	DRIVE0	HOSTA	CTL0P0
MEDC	DRIVE0	HOSTA	CTL0P0
MEDD	DRIVE0	HOSTB	CTL0P0
MED E	DRIVE0	HOSTB	CTL0P0

## フロントページの続き

(72)発明者 佐藤 雅彦  
神奈川県小田原市国府津2880番地株式会社  
日立製作所ストレージシステム事業部内  
(72)発明者 村岡 健司  
神奈川県小田原市国府津2880番地株式会社  
日立製作所ストレージシステム事業部内

(72)発明者 高木 賢一  
神奈川県小田原市国府津2880番地株式会社  
日立製作所ストレージシステム事業部内  
(72)発明者 小林 正明  
神奈川県小田原市国府津2880番地株式会社  
日立製作所ストレージシステム事業部内

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**